

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

SURGICAL INSTRUMENT SERVICE  
COMPANY, INC.,

*Plaintiff/Counter-Defendant,*

v.

INTUITIVE SURGICAL, INC.,

*Defendant/Counterclaimant.*

Case No. 3:21-cv-03496-VC

Honorable Vince Chhabria

**EXPERT REPORT OF KURT HUMPHREY**

Complaint Filed: May 10, 2021

**Highly Confidential – Subject to Protective Order**

**TABLE OF CONTENTS**

I. QUALIFICATIONS .....	1
II. PRIOR TESTIMONY AND PUBLICATIONS.....	2
III. ENGAGEMENT AND COMPENSATION .....	4
IV. SUMMARY OF OPINIONS.....	4
V. ENCRYPTION OF X AND XI ENDOWRISTS IS SUBSTANTIALLY MORE DIFFICULT TO REVERSE ENGINEER THAN SI, BUT IS NONETHELESS A MATTER OF AVAILABLE COMPUTING AND ENGINEERING RESOURCES .....	5
VI. INTUITIVE’S REASON FOR EMPLOYING THE MORE ROBUST ENCRYPTION AND SECURITY FEATURES FOR THE X AND XI ENDOWRISTS WAS TO PREVENT MODIFICATION OF THE USE COUNTER .....	15
VII. CONCLUSION .....	26

## **I. QUALIFICATIONS**

1. I currently work as Managing Director and Principal Technologist at IP Engenuity LLC. I have held that position for the past 17 years.

2. I hold B.S. and M.S. degrees in Ceramic Engineering from the University of Missouri-Rolla and worked primarily as a Process Development Engineer and Process Integration Manager during my 20+ year history in integrated circuit (IC) device and smart sensor processing. My professional experience in industry included responsibilities for complementary metal oxide semiconductor (CMOS) process development for DRAM, SRAM, EEPROM and SONOS flash and embedded non-volatile (NV) memories at AT&T Technologies, Philips Research Laboratories in Eindhoven, NL, and United Technologies Microelectronics Center. While at Philips, I collaborated with engineers at Siemens (DE), IBM (US), Intel (US), Motorola (US), Texas Instruments (US) and SEMATECH (US) on next-generation memory technology through formal technology transfer agreements with Philips (NL).

3. I am an expert in reverse engineering (RE) industrial and consumer microelectronic devices, components and systems including RFID products such as smart EMV smartcards and other proximity integrated circuit cards (PICCs). Over the course of my career, I have reverse engineered a large number and wide variety of semiconductor devices including microprocessors and non-volatile memories such as EEPROMs and Flash products for OEMs such as Apple, Alcatel-Lucent (Nokia) and others.

4. I have been engaged by multiple clients to extract or “dump” contents of specific EEPROMs and flash memories used in contactless RFID smart cards such as Visa payWave, Gemalto and other contactless EMV cards. The primary objective was to analyze the code or firmware with respect to patent enforcement/infringement matters.

5. I have general familiarity with encryption and security used in RFID communications, including encryption via stream ciphers and mutual authentication protocols.

6. A copy of my current *Curriculum Vitae* is attached to this report at Attachment 1.

## II. PRIOR TESTIMONY AND PUBLICATIONS

7. I have been deposed as a technical expert nine times and provided expert trial testimony the following cases:

- a. I was engaged as an expert by Rebotix Repair LLC regarding reverse engineering and resetting of the use counter for Xi EndoWrists.<sup>1</sup> I was deposed in that matter.
- b. I was engaged as an expert by Hewlett Packard in an International Trade Commission (ITC) patent infringement case in 2006/2007 against Acer.<sup>2</sup> I provided reverse engineering and technical product testing services, prepared an expert report based on my empirical findings and was subsequently deposed.
- c. I was engaged as an expert by Clutch City Sports and Entertainment, L.P. in a matter against iLight Technologies, Inc.<sup>3</sup> I performed failure analyses on sample products, prepared an expert report, was deposed, and testified before a jury.
- d. I was engaged as an expert by General Access Solutions, LTD where I submitted an expert report and was deposed.<sup>4</sup>

---

<sup>1</sup> *Rebotix Repair LLC v. Intuitive Surgical, Inc.*, Case No. 8:20-cv-02274 (M.D. Fla)

<sup>2</sup> *Personal Computers and Digital Display Devices*, ITC Inv. No. 337-TA-606 (*Hewlett Packard v. Acer, Inc. et al.*)

<sup>3</sup> *Clutch City Sports & Entertainment, L.P. v. iLight Technologies, Inc. et al.*, Cause No. 2009-76645 (157<sup>th</sup> Dist. Ct., Harris County, TX Nov. 2009)

<sup>4</sup> *Sprint Spectrum L.P. v. General Access Solutions, LTD*, Case No. IPR2017-001889 (PTAB 2017)

- e. I was engaged as an expert by Proxense LLC in a patent infringement case involving Bluetooth Low Energy technology where I submitted an expert report regarding claim construction and was also deposed.<sup>5</sup>
- f. I was engaged by Neogen Corp. in a case where I provided an expert report, trial for which is scheduled for June 2022.<sup>6</sup>
- g. I was engaged by Ocean Semiconductor LLC in a case where I provided an expert declaration and was deposed.<sup>7</sup>
- h. I was engaged by Ocean Semiconductor LLC in a case where I provided an expert declaration and was deposed.<sup>8</sup>
- i. I was engaged by Ocean Semiconductor LLC in a case where I provided an expert declaration and was deposed.<sup>9</sup>
- j. I was engaged by Ocean Semiconductor LLC in a case where I provided an expert declaration and was deposed.<sup>10</sup>
- k. I was engaged by Ocean Semiconductor LLC in a case where I provided an expert declaration and was deposed.<sup>11</sup>

---

<sup>5</sup> *Proxense LLC v. Target Corporation*, Case No.6:20-cv-879 (W.D. Tex.)

<sup>6</sup> *Neogen Corp. v. Innovative Reproductive Technology LLC*, Case No. 4:19-cv-00330-RGE-CFB (S.D. IOWA)

<sup>7</sup> *Western Digital Technologies, Inc. v. Ocean Semiconductor LLC*, Case No. IPR Case IPR2021-00929 (PTAB 2021)

<sup>8</sup> *Applied Materials, Inc. v. Ocean Semiconductor LLC*, Case No. IPR2021-01340 (PTAB 2021)

<sup>9</sup> *Applied Materials, Inc. v. Ocean Semiconductor LLC*, Case No. IPR2021-01342 (PTAB 2021)

<sup>10</sup> *Applied Materials, Inc. v. Ocean Semiconductor LLC*, Case No. IPR2021-01344 (PTAB 2021)

<sup>11</sup> *ST Microelectronics, Inc. v. Ocean Semiconductor LLC*, Case No. IPR2021-01349 (PTAB 2021)

8. A list of all publications I have authored or co-authored during the past ten years is included in my *Curriculum Vitae*, attached to this report at Attachment 1.

9. I am listed as an inventor or co-inventor on the patents listed in Attachment 1.

### **III. ENGAGEMENT AND COMPENSATION**

10. I am submitting this report at the request of Haley Guiliano LLP, counsel for Surgical Instrument Service Company, Inc. (“SIS”), the named plaintiff in the lawsuit captioned on this report’s first page. This report sets forth opinions I have formed about which I may testify if called as a witness at the trial of this lawsuit.

11. I am an independent expert with extensive experience in reverse engineering, integrated circuits, and wireless communication systems including RFID systems. I have been asked to provide opinions about the encryption utilized on Intuitive Surgical Inc. (“Intuitive”) X and Xi EndoWrist products.

12. The facts and data I considered in connection with forming my opinions are identified in the body of this report and at the attached Attachment 2.

13. I am being compensated for my time spent in preparing this report at an hourly rate of \$450/hr. If asked to testify in this lawsuit, I will be compensated at the rate of \$450/hr for deposition testimony and \$450/hr for testifying at trial. My compensation does not depend in any way on the outcome of this action.

### **IV. SUMMARY OF OPINIONS**

14. The encryption on X and Xi EndoWrists requires substantially more computing resources to reverse engineer than the encryption of Si EndoWrists. Although the encryption techniques utilized by Intuitive for the use counters of the X and Xi EndoWrists can, and in fact have been, reverse engineered with adequate computing power and resources, as compared to the

encryption used for the use counter of the Si EndoWrists, the Xi encryption requires substantially more time and resources to reverse engineer.

15. Reverse engineering of the X and Xi EndoWrist encryption is simply a matter of computing power and financial resources. The time necessary to reverse engineer an X or Xi EndoWrist would be compressed with additional resources, and would have been possible within a similar time frame at least as early as 2019.

16. Intuitive's reason for employing encrypted communication between the X/Xi robots and the EndoWrists was to prevent modification of the use counter. The electronics within the Intuitive X and Xi EndoWrists do not actively control the EndoWrist, and third parties have only attempted to access or reverse engineer the use counter, not any other functionality of Si or X/Xi EndoWrists. Preventing third parties from accessing the use counter was Intuitive's primary concern when it selected the encryption used with Xi EndoWrists, and [REDACTED]

[REDACTED]

[REDACTED]

**V. ENCRYPTION OF X AND Xi ENDOWRISTS IS SUBSTANTIALLY MORE DIFFICULT TO REVERSE ENGINEER THAN Si, BUT IS NONETHELESS A MATTER OF AVAILABLE COMPUTING AND ENGINEERING RESOURCES**

17. I understand that Intuitive Surgical, Inc. manufactures and sells surgical robots under the da Vinci brand name and related surgical attachments/instruments under the EndoWrist brand name. Specifically, there are multiple models or generations of commercial da Vinci robots and EndoWrists at issue here, including the Intuitive IS2000 designated "S", IS3000 designated "Si", IS4200 designated "X" and IS4000 designated "Xi" robots and their corresponding S/Si and X/Xi EndoWrist attachments.<sup>12</sup>

---

<sup>12</sup> Deposition of Anthony McGrogan at 15:14-20

18. Of particular interest is the use counter incorporated into both S/Si and X/Xi generations of robots and corresponding EndoWrist instruments. For both S/Si and X/Xi platforms, the use counter is designed to track the number of times a particular EndoWrist has been used in surgery. Each EndoWrist use counter is pre-programmed by the manufacturer (Intuitive), prior to delivery to the customer, with a limited number of uses or “lives”.<sup>13</sup> According to Intuitive’s Vice President of Design Engineering, Mr. McGrogan, in describing the use counters, “The Gen 3 Si/S instruments, those use a Dallas chip, which is a hard-wire connection. And on Gen 4, which is X/Xi, we use an RFID counter.”<sup>14</sup> It is my understanding based on technical documentation that I have reviewed that the actual use counter is solely designed to track the number of times an instrument has been used in surgery and report the remaining use count to the robot in order to display the number of “Uses Remaining”.

19. In the Rebotix matter, I prepared and submitted an expert report entitled, “Expert Report of Kurt Humphrey,” dated July 26, 2021 (my “Rebotix Report”). In the Rebotix Report, I opined regarding the technology and methodology that Rebotix would use to access and reset the Xi use counter. I have reviewed my Rebotix Report (attached as Attachment 3) and the documents considered therein (listed at the last page), and adopt and incorporate that Rebotix Report, including the opinions it represents and the identifications of documents and exhibits I reviewed, in its entirety herein.

20. In my Rebotix Report, I discussed the use counter of the Si EndoWrists and the security techniques used to prevent third parties from modifying that use counter. Rebotix Report at ¶¶ 12, 31-35.

---

<sup>13</sup> Deposition of Anthony McGrogan at 20:8-17

<sup>14</sup> Deposition of Anthony McGrogan at 77:18-20



21. In my Rebotix Report, I also discussed the use counter of the X and Xi EndoWrists and the encryption techniques used to prevent third parties from modifying that use counter. Rebotix Report at ¶¶ 19-30, 36-43.

22. As I noted in my Rebotix Report, “[t]he primary difference between the EndoWrist usage counter on the da Vinci S/Si EndoWrist and the da Vinci Xi EndoWrist is the manner in which the usage counter is accessed by the da Vinci system. For the S/Si instruments, the da Vinci system reads the data on the usage counter via a hard-wire connection, and for the Xi instruments, the da Vinci robot reads the data on the usage counter via an RFID counter.”<sup>15</sup> Rebotix Report at ¶ 13.

23. The use counters of both S/Si and X/Xi EndoWrists are not based on anything about the use of the EndoWrist instrument during surgery, such as the time or amount of use during the surgery or forces incurred during surgery. In fact, although Intuitive measures, logs and stores detailed time-series logs of the torque on each of the motors and corresponding movement axes of the EndoWrists for both Si and Xi systems that would make such analysis possible,<sup>16</sup> it does not use this information in the use counter in any manner.<sup>17</sup>

24. On a da Vinci S/Si EndoWrist, the use counter is programmed into a Dallas Semiconductor chip hard-wired to the Gen 3 S/Si instrument. Specifically, a Dallas Semiconductor (DS) DS2505 16Kb Add-Only Memory chip is used in the S/Si EndoWrists. The DS2505 has three main memory components: a 64-bit lasered ROM, a 16384-bit EPROM Data Memory and a 704 bit EPROM Status Memory.<sup>18</sup> The S and Si instruments communicate with the

---

<sup>15</sup> Deposition of Anthony McGrogan at 77:12-23

<sup>16</sup> 30(b)(6) Deposition of Grant Duque at 13:11-18:23

<sup>17</sup> 30(b)(6) Deposition of Grant Duque at 18:25-19:10

<sup>18</sup> REBOTIX148555

EndoWrist via a one wire memory bus.<sup>19</sup> The DS2505 memory locations store the usage count data for the S and Si instruments. When the S/Si EndoWrist is connected to the da Vinci robot, the robot reads the data on the use counter through a hard-wire connection to determine how many uses remain on the counter. If the da Vinci robot reads that the EndoWrist has at least one use remaining, it will allow that EndoWrist to be used in surgery. In the event the use counter communicates that there are no uses remaining, the EndoWrist unit is rendered inoperable and the internal security key is deleted. According to Intuitive, “In comparison on IS3000 [S/Si robot] - ISI Key generated from Dallas unique id - key is needed for system to access Dallas data. When instrument is expired, key is wiped. All bits on dallas can only be ‘cleared,’ so once lives ticked off, cannot be reset.”<sup>20</sup>

25. The da Vinci X/Xi robots and EndoWrists, on the other hand, communicate remaining use counts via RFID. An RFID system is a method by which data is communicated between two sources.<sup>21</sup> A RFID system consists of two components: tags and readers. A reader is a device that includes antennas that can emit and receive RF signals from a tag and optionally power a passive RFID tag. The tag uses RF signals to communicate information to a reader.<sup>22</sup> Unlike a hardwire connection, the RFID tag can transmit data without physically being connected to the RFID reader.<sup>23</sup> There are two types of tags—passive and active.<sup>24</sup> A passive tag is powered

---

<sup>19</sup> Deposition of Stan Hamilton at 143:12-144:7

<sup>20</sup> Intuitive: IS4000 8mm Base Instruments Final Design Review (FDR) Slide 192; Intuitive-00544903, at 00545094.

<sup>21</sup> <https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification>

<sup>22</sup> <https://www.fda.gov/radiation-emitting-products/electromagnetic-compatibility-emc/radio-frequency-identification-rfid>

<sup>23</sup> <https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification>

<sup>24</sup> <https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification>

by the signal emitted from the reader.<sup>25</sup> An active tag is powered by a battery.<sup>26</sup> Each tag can store a range of information, from a single serial number to multiple pages of data.<sup>27</sup> An RF system for transmitting data does not affect the underlying stored data—it is a communication method for such data rather than a data storage system.

26. According to Intuitive’s user manuals for the da Vinci X and Xi systems, each system uses RFID communication to detect installed instruments.<sup>28</sup> The RFID communication between the X/Xi robot and Xi EndoWrists operates at 13.56 MHz and complies with ISO/IEC 14443 Type B.<sup>29</sup>

27. X/Xi instruments include an Atmel CryptoRF interface with Atmel CryptoMemory security features. I have reviewed the CryptoRF EEPROM Memory Full Specification datasheet.<sup>30</sup> By default the CryptoRF has no enabled security, and operates as a simple RFID EEPROM memory.<sup>31</sup> Intuitive has confirmed that the RFID tags used in the X/Xi EndoWrist instruments are passive RFID tags and are powered by the RFID reader in the X/Xi system.<sup>32</sup> Contrary to the unencrypted hardwired data communications between the EndoWrist’s Dallas chip and the S/Si robot, the user-configurable encrypted wireless data communications between the Atmel RFID

---

<sup>25</sup> <https://www.atlasrfidstore.com/rfid-insider/active-rfid-vs-passive-rfid>

<sup>26</sup> <https://www.atlasrfidstore.com/rfid-insider/active-rfid-vs-passive-rfid>,  
<https://www.rfidjournal.com/faq/whats-the-difference-between-passive-and-active-tags>

<sup>27</sup> <https://www.fda.gov/radiation-emitting-products/electromagnetic-compatibility-emc/radio-frequency-identification-rfid>

<sup>28</sup> Intuitive Surgical da Vinci Xi System User Manual at E-16 (Intuitive-00002502 at 786) (“RFID communication is used by the da Vinci Xi system to detect and identify instruments and endoscopes that are installed on the system.”) Intuitive Surgical da Vinci X System User Manual at E-11 (SIS357469 at 717) (“RFID communication is used by the system to detect and identify instruments and endoscopes that are installed on the system.”)

<sup>29</sup> Intuitive Surgical da Vinci Xi System User Manual at E-17 (Intuitive-00002502 at 787), Intuitive Surgical da Vinci X System User Manual at E-12 (SIS357469 at 718)

<sup>30</sup> SIS357309 - Atmel CryptoRF EEPROM Memory Full Specificati,

<sup>31</sup> SIS357309 at 411

<sup>32</sup> 30(b)(6) Deposition of Grant Duque at 22:5-21

chip and the X/Xi robot are inherently more difficult to capture and decrypt. For example, one lead Intuitive engineer explained:

- Q: And is it your understanding that there's different encryption used on the Si Dallas chip versus the Xi RFID chip?
- A: That is correct.
- Q: Is that the reason why at this time you believe that Xi is impossible?
- A: That is correct.<sup>33</sup>

28. As Intuitive explained in its “Instrument Security Analysis” of December 2019, the respective security of the S/Si is “Low” compared to the “Medium” security utilized in X/Xi:<sup>34</sup>

Product	Authentication chip	Interface	Counterfeit Auth Key	Use count	Security Level
Si	Dallas DS2505 (Production year ~1995)	1-wire	Passcode	OTP	Low
X/Xi/SP	Atmel AT88SC6416CRF (Production year ~2004)	RF	Secret Key	OTP	Medium

29. As Intuitive has explained, the main differences are that in the S/Si EndoWrists the “Communication Channel is not encrypted” and the “Master Key is hard coded and is not well protected in the system” whereas X/Xi EndoWrists have an “Authenticated and secure channel” and the “MasterKey is protected by CryptoCompanion”:<sup>35</sup>

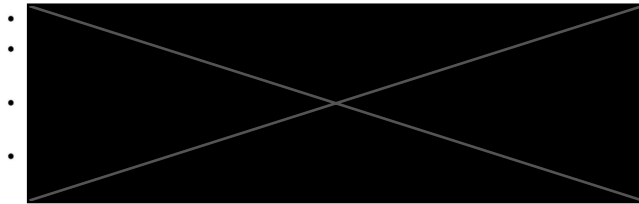
<sup>33</sup> Deposition of Shark Somayaji at 109:25-110:6

<sup>34</sup> Intuitive-01107582, at 583

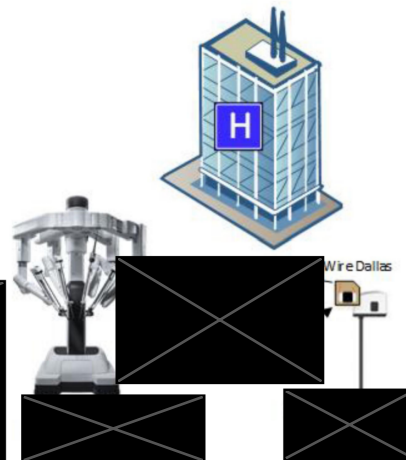
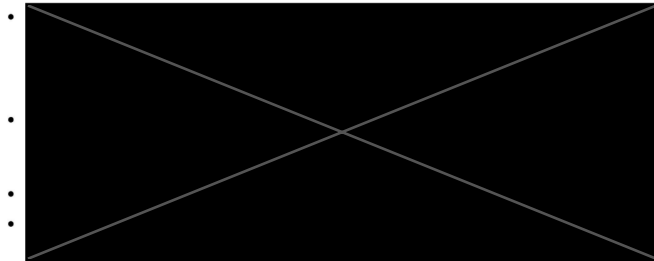
<sup>35</sup> Intuitive-01107582, at 584-585

## Si Instruments

- Authentication scheme

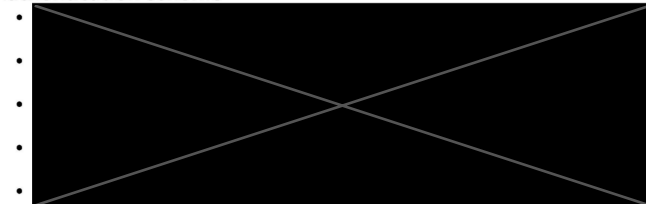


- Weaknesses

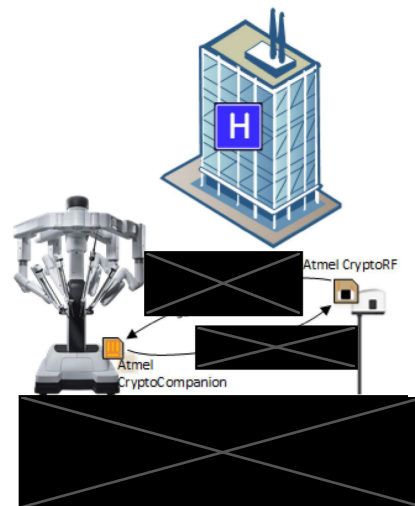
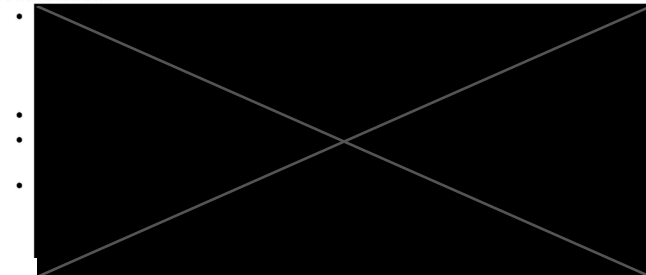


## X/Xi/SP Instruments

- Authentication scheme



- Weaknesses



30. These changes to the authentication and encryption methods used between the S/Si and X/Xi EndoWrists and systems substantially increase the amount of effort and computing power necessary to reverse engineer the X/Xi encryption, access and reset the use counter. Nonetheless, that does not mean that the X/Xi cannot be reverse engineered. For example, in October 2019, Intuitive was discussing third-party information that the Atmel “CryptoRF product

line we currently use is not as secure,” which raised concerns about “about methods to reprogram our RFID's, i.e. change the life-count so that instruments get re-used beyond their design life.”<sup>36</sup>

As one of Intuitive's engineers explained when discussing this e-mail chain:

- Q. Do you have an understanding of what it would be referring to to be hacking the chip you use?
- A. Yes.
- Q. What's your understanding?
- A. My understanding would be trying to break into the RFID chip and the encryption. End of the day, these are all encryptions. So encryptions have a computer limit, right? Like, there is processing power that's needed, and you have to try combinations. And I am thinking they are saying there's an opportunity to hack into our RFID chip. Doesn't mean it's done, but that's true for all cryptography, right? Like, any encryption can be end of the day broken.<sup>37</sup>

31. In my original Report, I opined that “an image will be extracted from the Atmel CryptoRF chip on the X/Xi EndoWrists by Rebotix,” that “based on Rebotix's past work with the S/Si EndoWrists and its understanding of the function of the usage counter, it will identify the usage counter in the extracted image,” and that “Rebotix will have the capability to implement a reset of the usage counter on the X/Xi EndoWrists.” Rebotix Report at ¶¶ 45-47.

32. Consistent with that opinion, Rebotix has now accomplished this from a technical perspective:

- Q. Has -- sitting here today, has Rebotix figured out how to circumvent the usage counter on Xi endoWrist instruments?

MR. ERWIG: Objection. Form.

THE WITNESS: Substantially, yes.

\* \* \*

- Q: So from a technical perspective today -- as of today, Rebotix has figured out how to reset the usage counter for Xi instruments. Is that what you're saying?

MR. CORRIGAN: Objection. Asked and answered.

MR. ERWIG: Same objection.

THE WITNESS: I agree. Yes. I answered.

---

<sup>36</sup> Intuitive-00999771 (Ex. 220 to Deposition of Shark Somayaji)

<sup>37</sup> Deposition of Shark Somayaji at 123:2-17

[REDACTED]

33. [REDACTED] Restore Robotics, [REDACTED]

[REDACTED] has created a reader for monitoring previously encrypted information of the EndoWrists, including the use count.<sup>39</sup>

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

<sup>38</sup> [REDACTED]

<sup>39</sup> Deposition of Kevin May at 50:7-16.

<sup>40</sup> Deposition of Kevin May, Exhibit 155 at Restore-0091199; Kevin May at 51:6-53:1.

<sup>41</sup> Deposition of Kevin May at 89:10-25.

<sup>42</sup> Deposition of Kevin May at 60:9-25.

<sup>43</sup> [REDACTED]

\_\_\_\_\_

— 100 —

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

[REDACTED]

[REDACTED]



<sup>44</sup> Deposition of Kevin May at 75:17-76:1.

<sup>45</sup> Deposition of Kevin May at 96:13-97:8.

46 



expensive. This reverse engineering work could have been performed at any time in the last five years, if not earlier, had the appropriate funding and resources been available.

**VI. INTUITIVE’S REASON FOR EMPLOYING THE MORE ROBUST ENCRYPTION AND SECURITY FEATURES FOR THE X AND Xi ENDOWRISTS WAS TO PREVENT MODIFICATION OF THE USE COUNTER**

37. It is reasonable to explore Intuitive’s possible motivation(s) in replacing the DS2505 EPROM with the Atmel CryptoRF EEPROM chip. After all, the old adage, “If it ain’t broke, don’t fix it” applies to complex systems, such as remote robotic surgical platforms, as much as it applies to other products including integrated circuit (IC) design, as demonstrated by the continued industrial interest in IP reuse. This philosophy is reflected in an excerpt from Exhibit 241, “Instruments for the S/Si and Xi platforms are similar in many regards. The materials used in the distal portion of the S/Si 8mm instruments are identical to those used in the equivalent versions of the Xi 8mm instruments.”<sup>47</sup> The key factors in making significant design or component changes to any product are generally associated with performance/reliability, availability, and/or cost.

38. In terms of performance, evidence has not been identified indicating that the Atmel RFID chip offers any substantive improvement over the existing DS2505 chip in operational performance of the X/Xi system. On the contrary, any possible, yet unstated, performance advantages that might have been anticipated by introducing the RFID chip were insignificant enough that Intuitive used the conventional Dallas chip as their contingency or back-up plan in the event the RFID chip design change failed. Figure 1 from Exhibit 265, indicates that the “Project (Technical/Schedule) Risks” associated with the RFID chip introduction were considered

---

<sup>47</sup> Deposition of Grant Duque, Exhibit 241 at Intuitive-00027299

“Medium” and that Intuitive’s RFID risk mitigation plan was to use the “Dallas chip as a “backup”.<sup>48</sup> Figure 1 is reproduced below for reference.

Project (Technical/Schedule) Risks (con't.)		
Item	Mitigation/Update	Risk
Increase engagement time	Reducing engagement time to 1.2 seconds by eliminating roll disc offset	Low
Earlier Failure from sine cycling	More testing/ investigate the root cause	High
RFID	Sterilization/life testing Reliability testing Dallas chip as a backup	Medium
Hypo-tube manufacturing	Alternate designs are being considered Improve manufacturing process Use IS3000 Hypo-tube	Medium

Figure 1

39. Moreover, another Intuitive slide from Exhibit 265 reproduced as Figure 2, below indicates that the X/Xi EndoWrist module was designed to use either the Dallas chip or the RFID chip without further modifications.<sup>49</sup> Therefore, it appears unlikely that the resulting EndoWrist operational or mechanical performance would be substantially different, or even distinguishable, regardless of which chip was used.

<sup>48</sup> 30(b)(6) Deposition of Grant Duque, Exhibit 265 at Intuitive-00542902 (Slide 107)

<sup>49</sup> 30(b)(6) Deposition of Grant Duque, Exhibit 265 at Intuitive-00542819 (Slide 24)

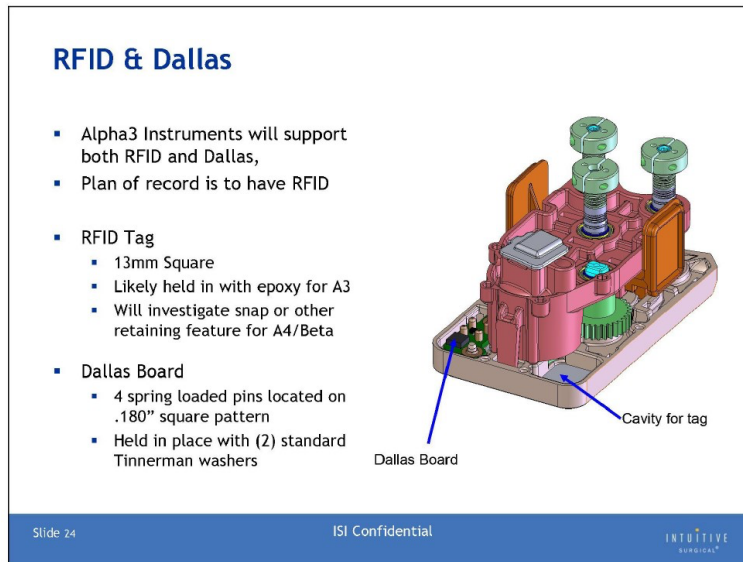


Figure 2

40. In terms of reliability, in reviewing the supplied the Intuitive documentation, there is no indication that a significant S/Si or EndoWrist instrument reliability issue associated with the Dallas chip was identified or addressed.

41. Moreover, a review of the disclosed comparative RMA/field failure data for the S/Si and X/Xi platforms provides no evidence of reliability issues associated with the DS2505 chip. Figure 3, the comparative “RMA Top Diagnoses by Rate” graphic from Exhibit 247, is reproduced below for reference.

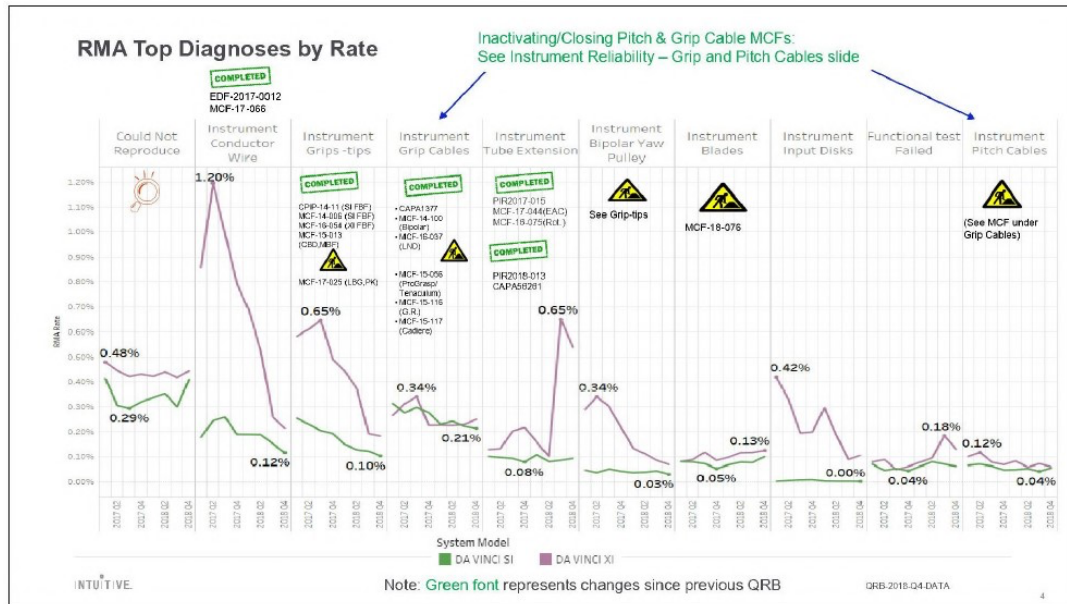


Figure 3

42. Although many factors can contribute to increased failure rates for a given product, it is interesting to note that Figure 1 shows 1) “Instrument Conductor Wire” failures were identified as the cause for a significantly higher Return Material Authorization (RMA) percentage for the “wireless” RFID Xi-EndoWrist instrument interface than for the “wired” Dallas Si-EndoWrist interface and 2) the return rate percentage for the Xi systems exceeds the return rate of the Si systems for essentially every RMA diagnosis. The disclosed RMA/return data details are insufficient to draw any firm conclusions regarding reliability issues associated with replacement of the DS2505 chip in the S/Si EndoWrist instruments with the Atmel CryptoRF chip in the X/Xi EndoWrist instruments but the results suggest that improved reliability was not a key factor or motivation in redesigning the X/Xi robot-EndoWrist interface.

43. In terms of availability, there is no evidence I am aware of indicating that the DS2505 device supply or availability was limited at the time of the X/Xi system design/development or would become threatened in the foreseeable future. On the contrary, as

discussed previously, the availability of Dallas chips was sufficient for Intuitive to plan to use the “Dallas chip as a backup” to mitigate risks associated with the development of the RFID interface for the X/Xi platform. Moreover, lack of adequate DS2505 chip supply would be particularly unlikely considering the relatively small number of DS2505 chips required to support typical S/Si and X/Xi EndoWrist production volumes. Therefore, migrating the DS2505 device from the S/Si platform to the X/Xi platform should have been relatively straightforward from an availability standpoint.

44. That leaves cost as the most likely motive for Intuitive to take on the substantial task of redesigning the X/Xi robot-EndoWrist interface. There are a variety of costs that can motivate businesses to consider redesigning their products. Three of the most common commercial costs are material, production, and opportunity, i.e. those impacting revenue or profit.

45. In the case of the S/Si and X/Xi systems, material cost is highly unlikely to be a factor in switching from the Dallas chip to the Atmel CryptoRF chip, since the difference in material costs of these commodity ICs is undoubtedly negligible compared to the cost of a da Vinci system and EndoWrist instruments used with the system.

46. Likewise, the difference in production cost associated with using either the Dallas chip or the Atmel RFID chip is also undoubtedly negligible. For example, Figure 2 above indicates the wired (Dallas) chip and wireless (RFID) chip are essentially interchangeable between the S/Si or X/Xi platforms. On the contrary, Intuitive documentation indicates that programming of the RFID chip requires special tooling that is not required for the programming of the Dallas chip.

47. Therefore, if reduced material costs and production costs are unlikely motivations to undertake the considerable effort/cost and risks associated with redesigning the X/Xi-EndoWrist interface, then one must consider opportunity costs as a possible motivation.

48. Review of the supplied Intuitive documentation sheds considerable light on the opportunity costs associated with redesigning the S/Si and X/Xi-EndoWrist instrument interface, namely in addressing lost revenues associated with used EndoWrist instrument repair and reprocessing by third-parties. For example, Intuitive's concern regarding third-party repair/reprocessing of used tools as it relates to the incorporation of the RFID chip is clearly evident an internal email entitled "RFID Team Action Items"<sup>50</sup>. The email begins with the statement,

"In my initial thoughts on this, there are two threats we're worried about:

1. Reprocessing: Take an expired instrument and restore its available lives
2. Counterfeiting: Take a non-ISI-designed instrument and put valid data on a tag so that it is accepted by our machine.

We'd like to make both of these difficult with the security features on our tag.

Reprocessing seems the more likely threat."

(Emphasis added).

49. Another excerpt from this same email, discussing Intuitive's primary concern of stopping additional lives from being added, states:

The unique id doesn't prevent reproprocessors from putting lives back on our instruments. In principle, you could copy the blob of data off a new instrument, then put that same blob of data back on once it's expired, and it will be as good as new. I believe the Dallas implementation uses a "write once" region in the tag to ensure that decremented lives stay decremented.

---

<sup>50</sup> 30(b)(6) Deposition of Grant Duque, Exhibit 267 at Intuitive-02068695-97.

(Emphasis added).

50. The “RFID Team Action Item” email continues by explaining that this is a reason to go with the Atmel solution:

“It seems to me that we want something to physically change in the tag (e.g., blowing a fuse) as we expire lives in the instrument. We do have something like that from Atmel. If we can't get it from Baylogh's tag suppliers, we would leave a pretty significant vulnerability.”

(Emphasis added).

51. Intuitive’s focus on using the Atmel chip for purposes of preventing the addition of more lives to the EndoWrists is demonstrated by another e-mail during early Xi EndoWrist development, in which an Intuitive lead engineer for “architectural decisions” and “high-level 2 strategy for design” for Xi<sup>51</sup> stated the sole concern as preventing addition of lives to the EndoWrist: “We need to at least make sure that someone can’t just copy the contents of a tag from a new instrument and reprogram it at the end of life with the same information.”<sup>52</sup>

52. Intuitive’s sole focus during encryption development on the use counter, and the opportunity cost of introducing encrypted communications for the use counter data is validated, for example, by Intuitive’s decision to phase out S/Si instruments, which was implicitly acknowledged to be to protect instrument revenue because “companies have so far only done reprogramming on Si.” and “And we probably have lead time before they figure out X/Xi.” as the reprogramming had not yet been reverse engineered for X/Xi.<sup>53</sup>

---

<sup>51</sup> 30(b)(6) Deposition of Grant Duque at 26:4-27:3

<sup>52</sup> 30(b)(6) Deposition of Grant Duque, Exhibit 266 (Intuitive-02068686)

<sup>53</sup> Intuitive-01019873

---

**From:** Katie Scoville [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=015E406D44CF40CDABB530EFD918CA54-KATIE SCOVIL]  
**Sent:** 5/7/2018 12:31:46 PM  
**To:** Ryan Shaw [Ryan.Shaw@intusurg.com]  
**Subject:** reprogrammed instruments and Si portfolio

Ryan,

Just thinking...the emergence of 3<sup>rd</sup> party reprogramming is another possible reason to move away from Si. The companies have so far only done reprogramming on Si. IF, they figure out Xi we have the ability to respond with SW much faster. And we probably have lead time before they figure out X/Xi. I don't think the slides need updating, but it is something to think about.

Thanks,  
Katie

**Katie Scoville**  
*Director Product Marketing, Secondary Markets*  
Office: +1 (408) 523-7562 Cell: +1 (408) 628-8323  
[katie.scoville@intusurg.com](mailto:katie.scoville@intusurg.com)

53. Therefore, the opportunity cost associated with a redesign of the X/Xi-EndoWrist interface using an encryption-capable RFID chip that will be more difficult to reset (such as by using the Rebotix Interceptor Assembly or similar technology), represents a substantial increase in Intuitive Surgical revenues. This would appear to be the strongest motivation to redesign the existing Dallas chip-based interface with the Atmel RFID interface.

54. Consistent with Intuitive's focus on preventing the addition of lives during X/Xi encryption development, Intuitive agrees that third parties have only ever attempted to access or reverse engineer the use counter.<sup>54</sup> Intuitive documentation and testimony indicate that third-parties have successfully reverse engineered, or attempted to reverse engineer, the S/Si and X/Xi robot/EndoWrist interfaces solely for the purpose of resetting the use counter to extend the life of the instrument.

---

<sup>54</sup> 30(b)(6) Deposition of Grant Duque at 34:2-35:22; Deposition of Shark Somayaji at 110:7-112:10





[REDACTED]

57. Yet, despite the [REDACTED]

[REDACTED]

[REDACTED]

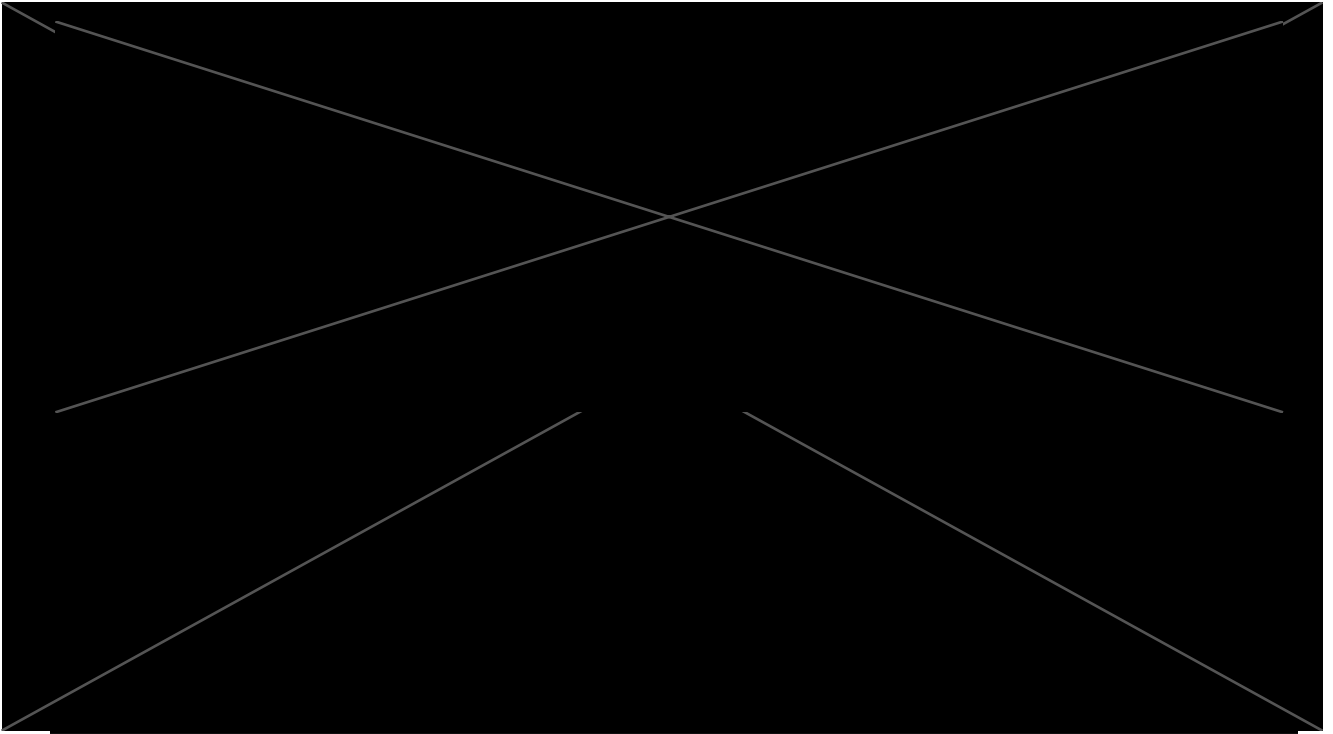
[REDACTED]

[REDACTED]<sup>57</sup>

---

<sup>56</sup> Deposition of Shark Somayaji at 132:8-138:2

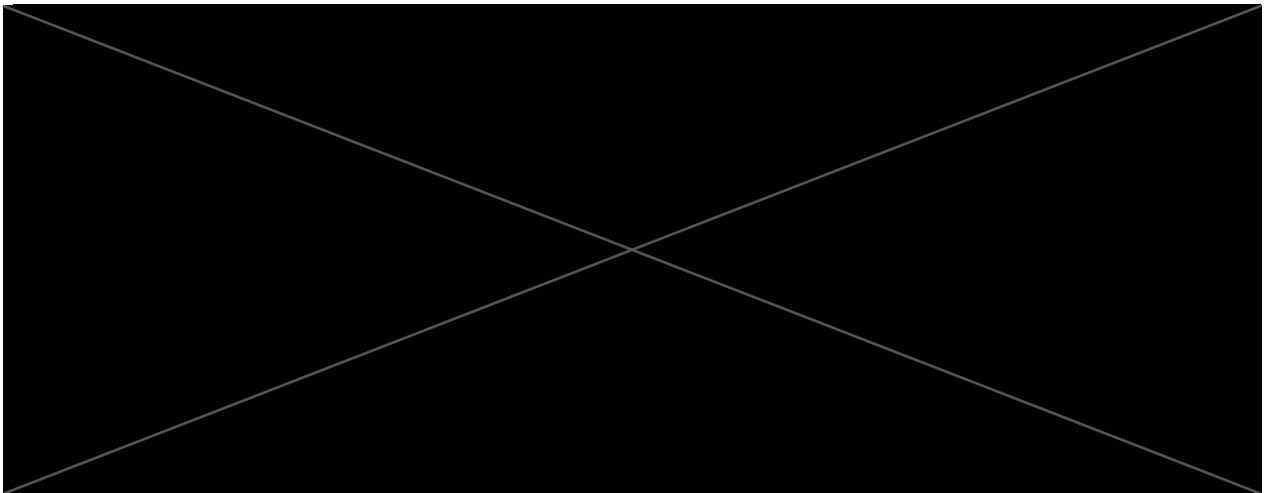
<sup>57</sup> Deposition of Shark Somayaji, Exhibit 228 at Intuitive-01004232, at 238.



58.

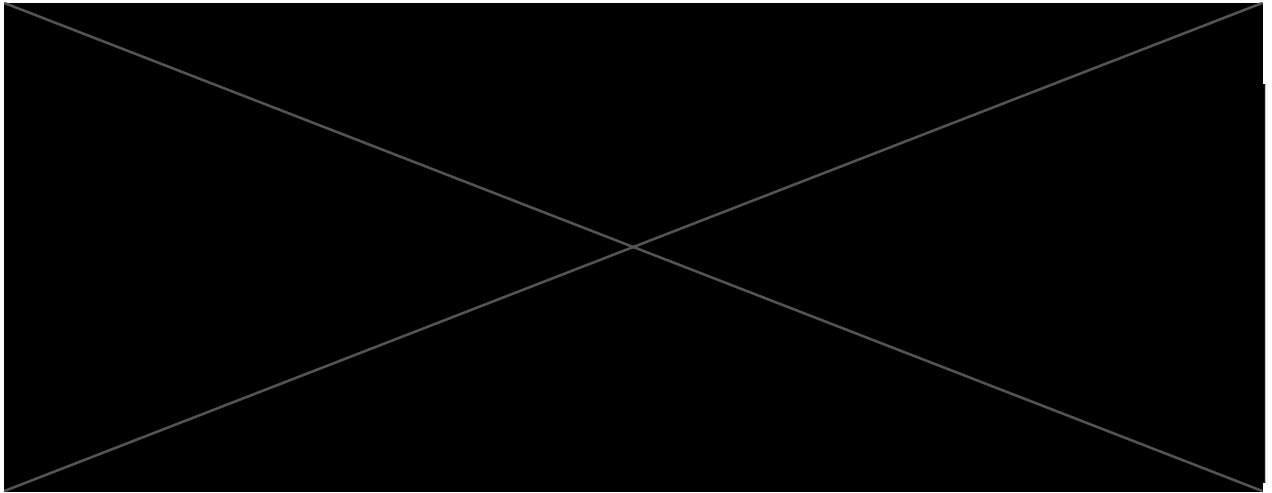
[REDACTED]

[REDACTED]



---

<sup>58</sup> Exhibit 228 at Intuitive-01004232, at 236, 239.



59. In sum, since the initial design of the encryption for the X/Xi EndoWrists in the early 2010s, Intuitive's driving concern with encryption has been to prevent extension of the number of instrument lives. Consistent with this driving concern, none of the other data stored within an EndoWrist has ever been accessed, and indeed, Intuitive admits that it would make no sense to access this other data. Intuitive's primary concern of stopping third-parties from adding lives to EndoWrists with X/Xi RFID encryption is further confirmed by the fact that [REDACTED]

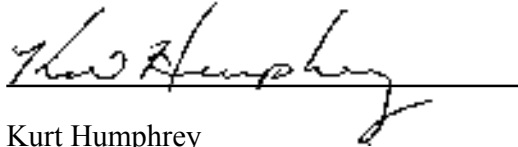
[REDACTED]

[REDACTED]

## VII. CONCLUSION

60. On balance, the Intuitive documentation and testimony I reviewed describing the design and development of the X/Xi-EndoWrist interface and the corresponding change from a wired, unencrypted Dallas chip (EPROM) to the wireless, encryption-enabled Atmel CryptoRF chip shows a deliberate attempt on the part of Intuitive to thwart efforts by third-parties to reset the instrument's use counter. Extending the field life of Intuitive's EndoWrist instruments, regardless of robotic platform, negatively impacts instrument sales resulting in a significant loss in revenue. Intuitive has been shown to have incurred additional design risks and costs in their development of the X/Xi robotic surgical platform and associated EndoWrist instruments in a

deliberate effort to thwart the instrument service providers' ability to reset the instruments' use counters and thereby extend the life of EndoWrist instruments.

A handwritten signature in black ink, appearing to read "Kurt Humphrey", is written over a horizontal line.

Kurt Humphrey

December 2, 2022

**ATTACHMENT 1**

***Curriculum Vitae* of Kurt Humphrey**

---

**Kurt D. Humphrey**

**Semiconductor Fabrication, Processing, and Chemical/Materials Expert**

After graduating with his B.S. in Ceramic Engineering, Mr. Humphrey accepted a Product Development engineering position with General Motors' AC Spark Plug division where he developed and patented the seminal process for physical vapor deposition (PVD) of Pt catalytic coatings on partially-stabilized zirconia oxygen sensors for state-of-the-art automotive emission control systems. Kurt was subsequently awarded a GM Graduate Study Fellowship and continued research in the area of automotive electronics with the development of **novel methods for fabricating multilayer ceramic capacitors** and other piezoelectric components through funding by General Motors Research Laboratories. After completing his M.S. degree in Ceramic Engineering, Kurt joined Delco Electronics (Delphi) Division of General Motors where he led process development and engineering in the areas of Czochralski (Cz) single-crystal silicon growth and semiconductor device/IC fabrication for bipolar, MOS, and silicon MEMS (MAP sensor) products.

Mr. Humphrey's expertise in materials and microelectronics subsequently led to assignments as Thin Films Process Development Manager where he developed and transferred to production the PVD tantalum salicide (TaSi) process used in AT&T's and Bell Labs' DRAM memory products. Kurt subsequently served as Submicron Process Integration Manager at N.V. Philips Research Laboratories in Eindhoven, NL including development of next-generation wafer cleaning, isolation, contact plug, via metallization and ILD gap-fill processes for state-of-the-art semiconductor device production. While at Philips, Kurt collaborated with engineers at AMD, Intel, TSMC, Texas Instruments, and Siemens on advanced materials development and IC process/fabrication technology through formal technology transfer agreements between the companies.

Mr. Humphrey came to Colorado Springs as Process Integration Manager for United Technologies Microelectronics Center (UMTC) developing and patenting state-of-the-art radiation-hardened triple-level metal (TLM) CMOS, programmable amorphous silicon anti-fuse, and deep-trench fully-isolated, complimentary bipolar silicon-on insulator (SOI) process technologies. Kurt transferred to Rockwell Semiconductor Systems/Conexant where he served as Advanced Process Integration Manager for 90nm CMOS pilot production. Later, with Rockwell and Conexant, Kurt developed and patented a commercial stiction-free wet etching process for releasing bulk micro-machined MEMS resonating structures used in state-of-the-art MEMS gyroscopes. During his long tenure in the industry, Mr. Humphrey worked with key semiconductor equipment and materials vendors including Applied Materials, Advantest, ASML, Ericsson, Huawei, JSR, Nokia, LAM, Novellus, ULVAC, SOITEC, Shin Etsu (SEH), Sumitomo, Teradyne and many others to develop and characterize next-generation microelectronic components, designs, and fabrication technologies.

Kurt has spent the past 22 years as a full-time IP technologist and subject matter expert (SME) in microelectronics and wireless telecom technologies. Kurt has served as a consulting and/or testifying expert in multiple lawsuits including an **ITC patent infringement case between HP and Acer and provided trial testimony as the expert for the plaintiff (the Houston Rockets organization) v. iLight Technologies in a 2012 product liability case involving LED lighting technology in 2012**. The jury found for the Plaintiff. Most recently, Kurt has provided expert analyses, reports and declarations in support of wireless telecom IPRs instituted by the USPTO's Patent Trial and Appeal Board (PTAB). Mr. Humphrey has been engaged numerous times to provide forensic/reverse engineering services and subject matter expertise primarily in the areas of commercial and industrial electronics and high-tech materials, and has analyzed literally thousands of patents and countless patent portfolios for clients in the Global High-tech Top 100.

**In addition to his consulting work, Mr. Humphrey currently serves as Adjunct Professor of Chemistry in the College of Engineering at Colorado Technical University teaching inorganic and organic chemistry.**

---

**PROFESSIONAL EXPERIENCE****IP Enginuity LLC.****2005-Present**

Managing Director/Principal Technologist

- Comprehensive Engineering Services Provider for the Intellectual Property and Patent Asset Management, Licensing, Litigation and Technology Transfer Industries.
- Prepare strategies and manage engineering services relating to IP asset and patent evaluation; reverse/forensic engineering and re-engineering; patent enforcement, assertion and licensing; portfolio mining; prior art searches; technology transfer; and IP litigation support.
- Primary technical contributor on projects relating to MCT/CZT IR focal plane arrays for the United Technologies Science Center, semiconductor devices and advanced/engineered materials including forensic and patent infringement investigations into LED lighting systems, LED phosphors, and solid-state DFB laser devices, organic LEDs (OLEDs) and optical networking components, protocols and standard essential patents (SEPs), consumer electronics, RFID, photonics and opto-electronic devices; MEMS and sensors; flat panel displays (FPDs), and biotech/medical products and systems.
- Expert witness experience in patent infringement, trade secret and antitrust litigation.

**TAEUS International Corp.****1999 – 2005**

Director, Engineering Services

- Managed patent evaluation and reverse engineering projects from the initial proposal through project completion and final review.
- Serve as a primary technical contributor/SME on wireless telecom/networking standards incl. 802.11, Bluetooth and 3G/4G cellular and associated SEPs, optical networking and opto-electronic/photonics components including collaboration with Dartmouth and HP scientists to measure and characterize non-linear optical effects in commercial optical fibers. Also as an SME on a variety of compound semiconductor devices, solid state DFB/quantum well lasers, photonics/opto-electronics components, FPD technologies, e.g. LCD, plasma and LED/OLED, , MEMS, sensors,) etc. and biotech related projects.
- Specific responsibilities include client interface, project definition, cost, resource and schedule planning, technical input, supervision of staff engineers, external consultants and labs, patent evaluation, claim chart construction, and technical report writing.
- Clients included many Global 100 high tech companies and leading U.S. patent law firms.

**Rockwell Semiconductor Systems/Conexant Systems****1995 - 1999**

Advanced Process Development Manager

- Assess new business opportunities, perform technical audits and generate comprehensive business and financial plans for review and approval by Rockwell CEO and senior staff.
- Primary focus on state-of-the-art semiconductor products e.g., Power-Trench Diodes and Trench IGBTs, CMOS imagers and MEMS gyros.
- Coordinate design rules, mask/reticle specifications, test chip design/layout, process qualification and transfer to production for 90nm CMOS process development in Rockwell's Advanced Process Technology (APT) department in Newport Beach.

Process Integration Manager

- Demonstrated first fully-functional Trench IGBTs and silicon MEMS gyro using 125mm substrates.
- Authored 3 MEMS and 1 SAW filter disclosures; 1 MEMS patent issued, others pending.
- Successful completion of comprehensive STI and 90nm CMOS process development test chips in record time to support an aggressive 90nm qualification schedule.



**United Technologies Corp. (UTMC)****1989 – 1995**

## Process Integration Manager

- Direct next-generation CMOS and bipolar process technology development. Development projects included: ACUTE (advanced dielectrically-isolated, complementary bipolar linear array process on SOI), UTERPROG ( radiation-hardened 1.0 $\mu$  CMOS PAL technology utilizing vertical amorphous Si antifuses), and UTERTLM (1.0 $\mu$  triple-level metal, rad-hard CMOS)
- Developed advanced amorphous silicon metal-to-metal antifuse technology to support 256k RHPROM and RHPAL field programmable products; 2 patents issued.
- Developed novel trench-isolated, complementary bipolar SOI process, 1 patent issued

**Philips Research Labs (Eindhoven, The Netherlands)****1986 – 1989**

## Process Integration Manager

- Direct development of 0.7 $\mu$  CMOS process from R&D phase through final product qualification as part of the Philips/Siemens “Mega” project. Project deliverables included commercial 1M SRAM and 4M DRAM products.
- Directed activities of 10 senior technologists.
- Developed first sub-micron CMOS process utilizing retro-wells, suppressed-BB LOCOS, salicide with TiSi<sub>2</sub> local interconnect, W plugs and I-line lithography.
- Integration team produced Philip's first fully-functional 1M SRAM using state-of-the-art 0.7 $\mu$  CMOS process (C1DM)

**AT&T Technologies****1983 – 1986**

## Process Engineering and Yield Enhancement Manager

- Coordinate DRAM process transfer from R&D to fab, and direct yield enhancement activities for 256k DRAM production in new 125mm line (KC-1).
- Section Leader for Thin Films/Ion Implantation Engineering
- Key contributor in successful start-up of new 125 mm high volume memory fab (KC-1);
- Representative on corporate committee for thin film metallization processes and invited speaker at SEMI/ASTM meeting on PVD target specifications.

**DELCO Electronics Div. General Motors****1980 – 1983**

## Process Development Engineer (Silicon Crystal Growing, Bipolar and MOS Fabs)

- Provide production engineering support, initially for Si crystal growing area, and later for MOS diffusion and LPCVD areas
- Evaluated external silicon wafer suppliers and introduced intrinsic-gettered substrates into MOS fab resulting in an average 7% increase in die yield across all devices

**AC Spark Plug Div., General Motors****1978 – 1980**

## Associate Process Development Engineer

- Developed process for depositing Pt catalytic thin films onto partially-stabilized zirconia oxygen sensors
- Key investigator and inventor on U.S. patent: “Electrode Sputtering Process for Exhaust Gas Oxygen Sensor”
- 1979 GM Graduate Study Fellowship Award

**EDUCATION and ACADEMIA**

M.S. Ceramic Engineering, University of Missouri - Rolla

B.S. Cum Laude, Ceramic Engineering, University of Missouri – Rolla

Adjunct Professor of Chemistry in the College of Engineering at Colorado Technical University-Colorado Springs - Current

**U.S. PATENTS:**

6,337,027 Microelectromechanical device manufacturing process

5,759,876 Method of making an antifuse structure using a metal cap layer

5,658,819 Antifuse structure and process for manufacturing the same

5,344,785 Method of forming high speed, high voltage fully isolated bipolar transistors on a SOI substrate

4,253,931 Electrode sputtering process for exhaust gas oxygen sensor

**HONORS**

General Motors Graduate Study Fellowship – 1979

United Technologies Silver Quill Award – 1994

Rockwell Outstanding Achievement Award – 1998

**PROFESSIONAL MEMBERSHIPS**

Institute for Electrical and Electronics Engineers (IEEE) / Electron Devices Society

Colorado Photonics Industry Association

Licensing Executive Society (LES)

Intellectual Property Owners Association (IPO)

Society for Optical Engineering (SPIE)

Intellectual Asset Management (IAM)

**Expert Litigation Case History (Partial)**

2007 – ITC Case No. 337-TA-606, *Hewlett Packard (Plaintiff) v. Acer International*:  
Provided expert reverse engineering services, expert report and deposition for the Plaintiff

2012 – District Court 157<sup>th</sup> Judicial District Harris County Texas Cause No.2009-76645, *Clutch City Sports and Entertainment a.k.a. Houston Rockets (Plaintiff) v. iLight Technologies*:  
Provided expert failure analysis services, expert report, deposition and trial testimony for the Plaintiff. Jury chose in favor of the Plaintiff.

2018 – IPR Case IPR2017-001889 before the USPTO PTAB, *Sprint Spectrum v. General Access Solutions (Patent Owner)*:  
Provided expert declaration and was deposed on behalf of the Patent Owner

2020 - IPR Case IPR2019-01668 before the USPTO PTAB, *Samsung Display (Petitioner) v. Solas OLED (PO)*: Provided expert declaration in support of the Patent Owner

2021 – Western District of Texas Civil Action No.: 6:20-cv-879 (ADA), *Proxense LLC (Plaintiff) v. Target Corp.*: Provided expert declaration and deposed on behalf of the Plaintiff

2021 - Middle District of Florida, Tampa Division, Case No. 8:20-cv-02274, *Rebotix Repair LLC (Plaintiff) v. Intuitive Surgical, Inc.*:  
Provided expert report and expert deposition on behalf of Plaintiff

2021 – Southern District of Iowa Central Division, Case No. 4:19-cv-00330-RGE-CFB, *Neogen Corp. v. Innovative Reproductive Technology LLC*: Provided expert report, scheduled for trial testimony in June

- 
- 2022 – IPR Case IPR2021-00929 (US 7,080,330) before the USPTO PTAB, *Western Digital Technologies, Inc.(Petitioner) v. Ocean Semiconductor LLC (Patent Owner)*: Provided expert declaration and was deposed on behalf of the Patent Owner
- 2022 – IPR Case IPR2021-01339 (US 8,686,538) before the USPTO PTAB, *Applied Materials, Inc.(Petitioner) v. Ocean Semiconductor LLC (Patent Owner)*: Provided expert declaration and was deposed on behalf of the Patent Owner
- 2022 – IPR Case IPR2021-01340 (US 6,725,402) before the USPTO PTAB, *Applied Materials, Inc.(Petitioner) v. Ocean Semiconductor LLC (Patent Owner)*: Provided expert declaration and was deposed on behalf of the Patent Owner
- 2022 – IPR Case IPR2021-01342 (US 6,968,248) before the USPTO PTAB, *Applied Materials, Inc.(Petitioner) v. Ocean Semiconductor LLC (Patent Owner)*: Provided expert declaration and was deposed on behalf of the Patent Owner
- 2022 – IPR Case IPR2021-01344 (US 6,907,305) before the USPTO PTAB, *Applied Materials, Inc.(Petitioner) v. Ocean Semiconductor LLC (Patent Owner)*: Provided expert declaration and was deposed on behalf of the Patent Owner
- 2022 – IPR Case: IPR2021-01349 (US 6,420,097) before the USPTO PTAB, *ST Microelectronics, Inc. (Petitioner) v. Ocean Semiconductor LLC (Patent Owner)*: Provided expert declaration on behalf of the Patent Owner.

**ATTACHMENT 2**

**List Of Materials Cited**

The following materials were used in forming my opinions:

1. Email thread beginning on December 10, 2021, filed as Doc. 180-1, Rebotix Repair, LLC re Document Number CPT2000126
2. Intuitive-00002502
3. Intuitive-00027298
4. Intuitive-00027299
5. Intuitive-00027622-24
6. Intuitive-00027843
7. Intuitive-00027844-46
8. Intuitive-00089606-08
9. Intuitive-00105113-18
10. Intuitive-00194931-35
11. Intuitive-00214902-03
12. Intuitive-00290826-31
13. Intuitive-00506505-641
14. Intuitive-00512348-53
15. Intuitive-00542796-919
16. Intuitive-00544903-5124
17. Intuitive-00552745-59
18. Intuitive-00555960
19. Intuitive-00556188-90
20. Intuitive-00556193-95
21. Intuitive-00556951-53
22. Intuitive-00560955-56
23. Intuitive-00561044-49
24. Intuitive-00561050-55
25. Intuitive-00593443-80
26. Intuitive-00602553-56
27. Intuitive-00602580
28. Intuitive-00602581
29. Intuitive-00602758-59
30. Intuitive-00602760-79
31. Intuitive-00671020-35
32. Intuitive-00960492-95
33. Intuitive-00967509
34. Intuitive-00967510-42
35. Intuitive-00967590

36. Intuitive-00967609-13
37. Intuitive-00967614-34
38. Intuitive-00988310-16
39. Intuitive-00990665-66
40. Intuitive-00991239-40
41. Intuitive-00991241-42
42. Intuitive-00994614-17
43. Intuitive-00999076
44. Intuitive-00999252-68
45. Intuitive-00999731-42
46. Intuitive-00999734
47. Intuitive-00999771-75
48. Intuitive-01001554-55
49. Intuitive-01002987-89
50. Intuitive-01004230-31
51. Intuitive-01004232-39
52. Intuitive-01005095-96
53. Intuitive-01019873
54. Intuitive-01031408-11
55. Intuitive-01085683-85
56. Intuitive-01095425-29
57. Intuitive-01107582-88
58. Intuitive-02066979-7059
59. Intuitive-02067770-72
60. Intuitive-02068686
61. Intuitive-02068695-97
62. REBOTIX148555-78
63. REBOTIX175417
64. REBOTIX175468
65. REBOTIX175710
66. Restore-00001248-56
67. Restore-00091199-206
68. Restore-00091362
69. Restore-00094918-56
70. SIS357469-812
71. SIS357309-468 - Atmel CryptoRF EEPROM Memory Full Specification
72. Expert Report of Kurt Humphrey, submitted in the matter of Rebotix Repair LLC v. Intuitive Surgical, Inc., Case No. 8:20-cv-02274 (M.D. Fla.) and dated July 26, 2021
73. Interview with Stan Hamilton on July 23, 2021
74. Deposition of Anthony McGrogan dated June 7th ,2021

75. Deposition of Stan Hamilton dated June 4, 2021
76. Expert Report of Gwen Mandel dated July 26, 2021
77. Fukami, Aya, et al., A New Model for Forensic Data Extraction from Encrypted Mobile Devices, *Forensic Science International: Digital Investigation*, Elsevier, May 27, 2021, [www.sciencedirect.com/science/article/pii/S2666281721000779](http://www.sciencedirect.com/science/article/pii/S2666281721000779).
78. Conti, Gregory, et al., Visual Reverse Engineering of Binary and Data Files, *Visualization for Computer Security Lecture Notes in Computer Science*, Sept. 2008, pp. 1–17., doi:10.1007/978-3-540-85933-8\_1.
79. A. Amsler and S. Shea, RFID (Radio Frequency Identification), TechTarget, <https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification>
80. 30(b)(6) Deposition of Grant Duque dated November 8, 2022
81. Exhibit 264 to the 30(b)(6) Deposition of Grant Duque dated November 8, 2022
82. Exhibit 238 to the Deposition of Grant Duque dated November 8, 2022
83. Deposition of Grant Duque dated November 8, 2022
84. Deposition of Sharathchandra “Shark” Somayaji dated November 4, 2022
85. Deposition of Kevin May dated November 3, 2022
86. Deposition of Stan Hamilton dated November 4, 2022

**ATTACHMENT 3**

**Expert Report of Kurt Humphrey in *Rebotix Repair LLC v. Intuitive Surgical, Inc.*, Case No. 8:20-cv-02274 (M.D. Fla)**

**UNITED STATES DISTRICT COURT  
MIDDLE DISTRICT OF FLORIDA  
TAMPA DIVISION**

REBOTIX REPAIR LLC,

Plaintiff,

VS.

INTUITIVE SURGICAL, INC.,

Defendant.

Case No. 8:20-cv-02274

HIGHLY CONFIDENTIAL  
INFORMATION - ATTORNEYS' EYES  
ONLY

## EXPERT REPORT OF KURT HUMPHREY



HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

**TABLE OF CONTENTS**

I.	Introduction.....	1
A.	Qualifications.....	1
B.	Documents Reviewed .....	2
C.	Compensation .....	3
II.	Background.....	3
A.	Da Vinci S/Si EndoWrists .....	4
B.	General Overview of RFID Systems .....	5
C.	The Atmel CryptoRF Family on the Da Vinci X/Xi System.....	5
D.	Rebotix Repair LLC's da Vinci S/Si Repairs .....	9
E.	Status of X/Xi Repairs .....	12
III.	Opinions.....	15
A.	Summary of Opinions.....	15
B.	An image will be extracted from the Atmel CryptoRF chip on the X/Xi EndoWrists by Rebotix.....	16
i.	Overview of image extraction .....	16
ii.	Process of image extraction.....	16
iii.	Extraction from the Atmel CryptoRF chip on the da Vinci Xi EndoWrists. ....	17
iv.	RFID Method .....	18
v.	Hard Wire Method.....	18
C.	The usage counter in the extracted image will be identified by Rebotix.....	19
i.	Analyzing an extracted image .....	19
ii.	The extracted image from the Atmel CryptoRF chip.....	20
iii.	Ms. Mandel's investigation has identified the location of the usage counter .....	20
iv.	Several additional factors make the process of Rebotix's image analysis for the Xi EndoWrist CryptoRF chip easier than others that I have encountered in my career .....	21

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

D.	Rebotix can use the extracted image to reset the usage counter on da Vinci Xi EndoWrists .....	23
i.	There are two approaches to reset the usage counter on the Xi EndoWrist.....	23
ii.	RFID Connection Writing.....	23
iii.	Hardware Chip Replacement.....	25
IV.	Other issues .....	26
A.	Intuitive's own security testing.....	26

## **I. INTRODUCTION**

### **A. Qualifications**

1. I currently work as Managing Director and Principal Technologist at IP Engenuity LLC. I have held that position for the past 15 years.

2. I hold B.S. and M.S. degrees in Ceramic Engineering from the University of Missouri-Rolla and worked primarily as a Process Development Engineer and Process Integration Manager during my 20+ year history in integrated circuit (IC) device and smart sensor processing. My professional experience in industry included responsibilities for complementary metal oxide semiconductor (CMOS) process development for DRAM, SRAM, EEPROM and SONOS flash and embedded non-volatile (NV) memories at AT&T Technologies, Philips Research Laboratories in Eindhoven, NL, and United Technologies Microelectronics Center. While at Philips, I collaborated with engineers at Siemens (DE), IBM (US), Intel (US), Motorola (US), Texas Instruments (US) and SEMATECH (US) on next-generation memory technology through formal technology transfer agreements with Philips (NL).

3. I am an expert in reverse engineering (RE) industrial and consumer microelectronic devices, components and systems including RFID products such as smart EMV smartcards and other proximity integrated circuit cards (PICCs). Over the course of my career, I have reverse engineered a large number and wide variety of semiconductor devices including microprocessors and non-volatile memories such as EEPROMs and Flash products for OEMs such as Apple, Alcatel-Lucent (Nokia) and others.

4. I have been engaged by multiple clients to extract or “dump” contents of specific EEPROMs and flash memories used in contactless RFID smart cards such as Visa payWave, Gemalto and other contactless EMV cards. The primary objective was to analyze the code or firmware with respect to patent enforcement/infringement matters.

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

5. I have general familiarity with encryption and security used in RFID communications, including encryption via stream ciphers and mutual authentication protocols.

6. I have been deposed as a technical expert four times and provided expert trial testimony in a product liability case.

a. I was engaged as an expert in an International Trade Commission (ITC) patent infringement case in 2006/2007 between Hewlett Packard and Acer on behalf of HP. I provided reverse engineering and technical product testing services, prepared an expert report based on my empirical findings and was subsequently deposed. Investigation No. 337-TA-606.

b. I performed failure analyses on sample products, prepared an expert report, was deposed, and testified before a jury in a 2012 LED lighting product liability case between Clutch City Sports and Entertainment (Plaintiff) and iLight Technologies et al (Defendants) Cause 2009-76645.

c. I was deposed in support of an IPR instituted by USPTO PTAB in 2018 where I represented the patent owner. (Case IPR2017-001889 Sprint Spectrum v. General Access Solutions)

d. I was also deposed in an active patent infringement case involving Bluetooth Low Energy technology, Proxense LLC v. Target Corporation, Civil Action No.: 6:20-cv-879.

**B. Documents Reviewed**

7. I have reviewed the Complaint in this matter, deposition testimony, documents produced in this action, publicly available documents, and Gwen Mandel's expert report. I have also had conversations with and reviewed technical documentation provided by Stan Hamilton of Rebotix Repair LLC regarding the past S/Si and current Xi EndoWrist repair

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

investigations. A list of the materials I have reviewed is attached as Exhibit 1. If I become aware of new information, I may modify the information in this report or supplement my opinions.

**C. Compensation**

8. I am being compensated for my time in this matter at the rate of \$300 per hour. My compensation in this matter is not contingent on the content of my testimony or any outcome in this litigation.

**II. BACKGROUND**

9. I am aware that Intuitive Surgical manufactures da Vinci surgical robots and EndoWrist instruments. The EndoWrist instruments are designed to be attached to the da Vinci surgical robot, and include a use counter. There are different models and generations of the da Vinci robot. The relevant models for my analysis are the third generation robots S/Si robots and the fourth generation X/Xi robots. Intuitive developed a set of EndoWrists for each robot. The instruments developed for the Xi da Vinci robot also function with the X robot.<sup>1</sup>

10. The use counter is incorporated in a chip on each EndoWrist. Intuitive designed the usage counter such that it decrements one use when an EndoWrist instrument is used in surgery.<sup>2</sup> The actual usage counter is solely designed to track the number of times an instrument has been used in surgery and report the usage count to the robot to display the number of uses remaining on the instrument.<sup>3</sup>

---

<sup>1</sup> The Intuitive website describes the da Vinci X as having “the same arm architecture as the da Vinci Xi so that [the customer] can use the latest instruments” <https://www.intuitive.com/en-us/products-and-services/da-vinci/systems##>.

<sup>2</sup> McGrogan Deposition at 17:13 – 18:6.

<sup>3</sup> Intuitive-00512349, Intuitive-00552746.

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

11. It is my understanding that Rebotix Repair LLC currently repairs S/Si EndoWrists but does not currently repair X/Xi EndoWrists.<sup>4</sup>

**A. Da Vinci S/Si EndoWrists**

12. On a da Vinci S/Si EndoWrist, the use counter is programmed into a Dallas chip hard-wired to the Gen 3 S/Si instrument. Specifically, a Dallas Semiconductor (DS) DS2505 16Kb Add-Only Memory chip is used in the S/Si EndoWrists.<sup>5</sup> The DS2505 has three main data components: a 64-bit lasered ROM, a 16384-bit EPROM Data Memory and a 704 bit EPROM Status Memory.<sup>6</sup> The S and Si instruments communicate with the EndoWrist via a one wire memory bus.<sup>7</sup> The DS2505 memory bus stores the usage count data for the S and Si instruments. When the S/Si EndoWrist is connected to the da Vinci robot, the robot reads the data on the usage counter through a hard-wire connection to determine how many uses remain on the counter. If the da Vinci robot reads that the EndoWrist has a use remaining, it will allow that EndoWrist to be used in surgery.

13. The primary difference between the EndoWrist usage counter on the da Vinci S/Si EndoWrist and the da Vinci Xi EndoWrist is the manner in which the usage counter is accessed by the da Vinci system. For the S/Si instruments, the da Vinci system reads the data on the usage counter via a hard-wire connection, and for the Xi instruments, the da Vinci robot reads the data on the usage counter via an RFID counter.<sup>8</sup>

---

<sup>4</sup> Hamilton Deposition at 57:5-19, 230:22-25.

<sup>5</sup> Interview with Stan Hamilton.

<sup>6</sup> DS2505 Datasheet at 2.

<sup>7</sup> Hamilton Deposition at 143:12 – 144:7.

<sup>8</sup> McGrogan Deposition at 77:12-23.

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

**B. General Overview of RFID Systems**

14. An RFID system is a method by which data is communicated between two sources.<sup>9</sup>

15. A RFID system consists of two components: tags and readers. A reader is a device that includes antennas that can emit and receive RF signals from a tag and optionally power a passive RFID tag. The tag uses RF signals to communicate information to a reader.<sup>10</sup>

16. Unlike a hardwire connection, the RFID tag can transmit data without physically being connected to the RFID reader.<sup>11</sup>

17. There are two types of tags—passive and active.<sup>12</sup> A passive tag is powered by the signal emitted from the reader.<sup>13</sup> An active tag is powered by a battery.<sup>14</sup> Each tag can store a range of information, from a single serial number to multiple pages of data.<sup>15</sup>

18. An RF system for transmitting data does not affect the underlying stored data—it is a communication method for such data rather than a data storage system.

**C. The Atmel CryptoRF Family on the Da Vinci X/Xi System**

19. According to Intuitive's user manuals for the da Vinci X and Xi systems, each system uses RFID communication to detect installed instruments.<sup>16</sup> The RFID

<sup>9</sup> <https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification>.

<sup>10</sup> <https://www.fda.gov/radiation-emitting-products/electromagnetic-compatibility-emc/radio-frequency-identification-rfid>.

<sup>11</sup> <https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification>.

<sup>12</sup> <https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification>.

<sup>13</sup> <https://www.atlasrfidstore.com/rfid-insider/active-rfid-vs-passive-rfid>.

<sup>14</sup> <https://www.atlasrfidstore.com/rfid-insider/active-rfid-vs-passive-rfid>, <https://www.rfidjournal.com/faq/whats-the-difference-between-passive-and-active-tags>.

<sup>15</sup> <https://www.fda.gov/radiation-emitting-products/electromagnetic-compatibility-emc/radio-frequency-identification-rfid>.

<sup>16</sup> Intuitive Surgical da Vinci Xi System User Manual at E-16, "RFID communication is used by the da Vinci Xi system to detect and identify instruments and endoscopes that are installed on the system." Intuitive Surgical

## HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

communication between the X/Xi robot and Xi EndoWrists operates at 13.56 MHz and complies with ISO/IEC 14443 Type B.<sup>17</sup>

20. The RFID system on the X/Xi system includes an Atmel CryptoRF interface with Atmel CryptoMemory security features. I have reviewed the CryptoRF EEPROM Memory Full Specification datasheet.<sup>18</sup> By default the CryptoRF has no enabled security, and operates as a simple RFID EEPROM memory.<sup>19</sup>

21. The CryptoRF family has several security measures that can be implemented by the customer, including communications security for each User Zone, transport security, and password security. Briefly, the customer/user can opt for one of three communication security modes, namely, the default or “Normal” CryptoRF security mode which is no encryption whatsoever, the “Authentication Communication Security” mode which provides for password encryption only, and “Encryption Communication Security” mode which encrypts both passwords and user data.<sup>20</sup>

22. Based on my review of the Intuitive X and Xi user manuals, each system conducts a mutual authentication using a pre-shared key and the data transmitted between the da Vinci and the RFID tag is encrypted using a Secure Hash Algorithm.<sup>21</sup>

---

da Vinci X System User Manual at E-11: “RFID communication is used by the system to detect and identify instruments and endoscopes that are installed on the system.”.

<sup>17</sup> Intuitive Surgical da Vinci Xi System User Manual at E-17, Intuitive Surgical da Vinci X System User Manual at E-17.

<sup>18</sup> Atmel CryptoRF EEPROM Memory Full Specification

<sup>19</sup> Atmel CryptoRF EEPROM Memory Full Specification at 117.

<sup>20</sup> Atmel CryptoRF EEPROM Memory Full Specification at Appendix I – K.

<sup>21</sup> Intuitive Surgical da Vinci Xi System User Manual at E-17, Intuitive Surgical da Vinci X System User Manual at E-17.



## HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

23. Intuitive's own cybersecurity documentation indicates that "Communications between the RFID reader and tag are encrypted."<sup>22</sup> Intuitive also states that the "[d]ata on RFID tag are encrypted and password-protected," and that the "[e]ncryption key and use counting data areas on RFID tag are one-time programmable and cannot be modified once written."<sup>23</sup>

24. According to technical documentation from Intuitive, the Intuitive Surgical Xi system (IS4000) RFID encryption is based on the SHA-1 encryption.<sup>24</sup> This is a dated Secure Hash Algorithm standard that has been superseded by SHA-2 and SHA-3 and is no longer recommended for use due known cryptographic weaknesses. Although SHA-1 encryption remains non-trivial to break, it is notable that according to industry sources (ComputerWorld) in 2017, "Starting with version 56, released this month, Google Chrome will mark all SHA-1-signed HTTPS certificates as unsafe. Other major browser vendors plan to do the same."<sup>25</sup>

25. I have reviewed Gwen Mandel's work with the Atmel CryptoRF chip and her methodology of examining the security present on the chip. Based on Ms. Mandel's work and the CryptoRF datasheet, the CryptoRF encryption communication mode applies only to the encryption of data transferred, i.e. communicated, between the Atmel RFID chip and the X/Xi robot. Neither Authentication Communication nor Encryption Communication modes are active when the chip is idled and not communicating with a da Vinci X/Xi robot.<sup>26</sup>

---

<sup>22</sup> Intuitive-00506542.

<sup>23</sup> Intuitive-00506542.

<sup>24</sup> Intuitive: IS4000 8mm Base Instruments Final Design Review (FDR) Slide 192.

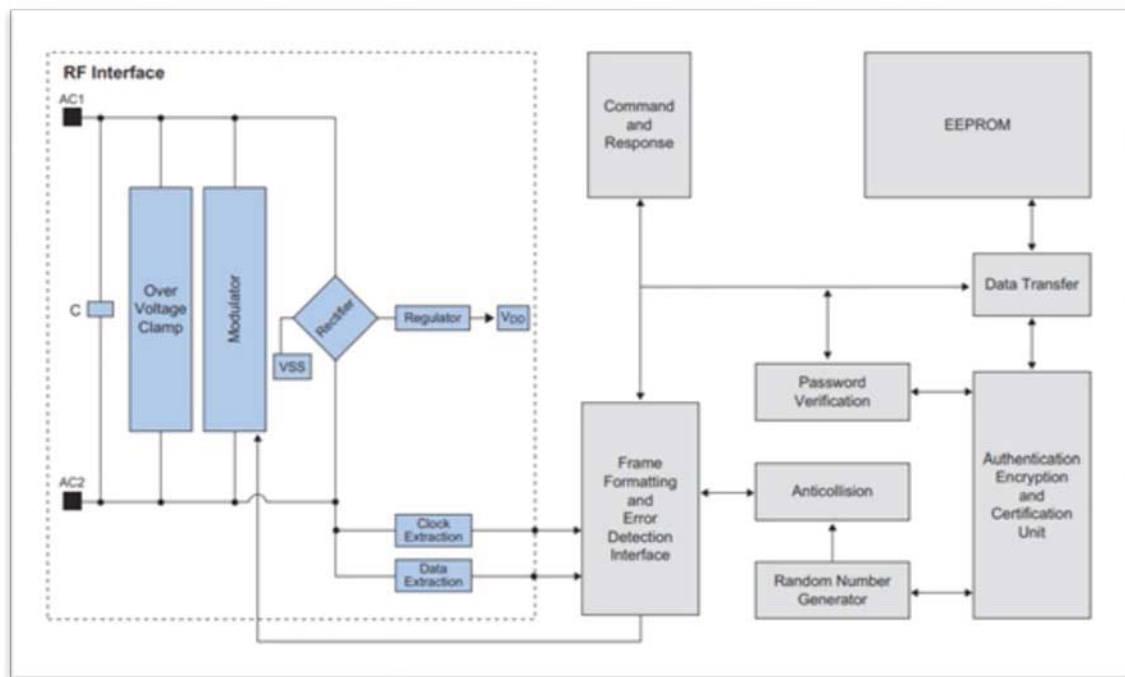
<sup>25</sup> ComputerWorld "The SHA1 hash function is now completely unsafe",  
<https://www.computerworld.com/article/3173616/the-sha1-hash-function-is-now-completely-unsafe.html>.

<sup>26</sup> Atmel CryptoRF EEPROM Memory Full Specification at Appendix I – K.

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

26. The Atmel CryptoRF chip consists of an RFID section/portion that is responsible for communicating via an RF link, and a separate section that contains all of the data that can be communicated via the RF link.<sup>27</sup>

27. The user data stored in the Atmel RFID chip can be optionally access and password protected but there is no provision for encrypting stored data internal to the EEPROM block. As previously stated, the only encryption capability available on the CryptoRF chip is during password transmission (through the Authentication Communication setting) and password/user data transmission (through the Encryption Communication mode).<sup>28</sup> The CryptoRF block diagram below supports this understanding as all data transferred in and out of the EEPROM block occurs via the data transfer block which is intermediary to the Authentication Encryption and Certification block.<sup>29</sup>



<sup>27</sup> Mandel Report at ¶¶ 9-14.

<sup>28</sup> Atmel CryptoRF EEPROM Memory Full Specification at Appendix I.

<sup>29</sup> Atmel CryptoRF EEPROM Memory Full Specification Fig. 1-1.

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

28. This comports with both Intuitive's description of the RFID security used by the X/Xi EndoWrists and my understanding of RFID security.

29. Based on my work with RFID technology and my familiarity with the Atmel CryptoRF chip, these security approaches only become active when the chip actually communicates with the robot. The EndoWrist CryptoRF chips are powered by the X/Xi robot reader through the chip's RF interface.<sup>30</sup> The CryptoRF datasheet states that the Authentication Communication and Encryption Communication modes remain in the designated security mode once active "until a security error occurs, a new Verify Crypto command is received, **RF power is removed**, or a DESELECT command or IDLE command is received."<sup>31</sup> (emphasis added). This means that the Atmel CryptoRF chip is unencrypted at rest.

30. Further, the chip can be easily removed from Xi EndoWrists for analysis.<sup>32</sup> Ms. Mandel was given ten chips from different models of EndoWrists that had been removed by Rebotix.<sup>33</sup>

**D. Rebotix Repair LLC's da Vinci S/Si Repairs**

31. It is my understanding that Rebotix Repair developed a method for resetting the usage counter on the da Vinci S/Si instruments. That process involves installing a small component on the EndoWrist called an Interceptor device.<sup>34</sup>

32. The Interceptor device allows Rebotix to reset the usage counter on individual EndoWrist instruments to its original number of uses.<sup>35</sup> When attached to the da Vinci

---

<sup>30</sup> Atmel Crypto RF EEPROM Memory Full Specification at 6 ("The RF interface powers the other circuits, no battery is required.")

<sup>31</sup> Atmel CryptoRF EEPROM Memory Full Specification at Appendix J-K.

<sup>32</sup> Interview with Stan Hamilton.

<sup>33</sup> Mandel Report at ¶ 17.

<sup>34</sup> Hamilton depo tr. 143:12-25.

<sup>35</sup> Hamilton depo tr. 143:12-25.

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

S/Si robot, the robot recognizes the instrument that has been repaired by Rebotix utilizing the Interceptor device and reads the number of uses remaining based on the reset use counter.

33. My understanding of the Rebotix Interceptor device development for the S/Si robot is based on my discussions with Rebotix engineers and review of relevant Rebotix technical documentation. In short, Rebotix developed the Interceptor device by:

- a. Monitoring the communications between the DS2505 memory chip on the EndoWrist and the S/Si robot.
- b. Analyzing changes in the DS2505 memory contents following many iterative operations using a variety of EndoWrist instruments. Analyzing the communications between the EndoWrist instruments and the S/Si robot provided Rebotix with essential information as to the format and nature of information being communicated between the EndoWrist and the robot.
- c. Performing and comparing DS2505 memory “dumps” prior to and following each EndoWrist operation allowed Rebotix engineers to map the DS2505 memory and identify the location where the use count was stored. An exemplary DS2505 memory map showing the location i.e. memory addresses, of the stored use counts, is included below for reference:

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
<b>LASER ROM</b>																
Dedicated location	DS2505 8-byte Serial Number															
<b>16Kbit USER MEMORY</b>																
	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
<b>0000-0070</b>	Copyright info															
<b>0080</b>	Copyright info cont'd					DS2505 Unique ID										0x02
<b>0090</b>																
<b>00A0</b>	EW Serial Number								Type Verify							
<b>00B0</b>				Ser # Verify												
<b>0C0-150</b>																
<b>0160</b>	EndoWrist Device Type															
<b>0170</b>	EndoWrist Device Type (cont'd)															
<b>0180</b>	Available Use Count (bitwise strike counter of remaining uses – MSB at address 0180 is last use)															
<b>0190</b>	Available Use Count (cont'd)															

d. comparison of the pre- and post- activity dumps in conjunction with communication information gathered from the 1-wire “sniffer” was used to correlate the data changes to specific activities and operations of the instrument including use count. Rebotix identified the portion of the data image that dealt with the usage counter. These reported techniques and results are consistent with conventional reverse engineering and forensic engineering methods that I have used throughout my career.

e. the extracted data and memory map of the S/Si instrument usage counter allowed Rebotix to develop a separate interface chip that would fulfill the same functions of the usage counter. As part of this process, Rebotix developed an understanding of the image on the S/Si usage counter chip and the manner in which the usage counter was coded into the memory of that chip.

34. The use of a bit-wise strike counter on the S/Si usage counter means that the uses on the S/Si counter could not be re-written/reset. A bit-wise strike counter does not allow values to be reset once the bits are struck. Moreover, according to Intuitive, the S/Si EndoWrist

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

included a security feature that “wiped” the ISI key used on the DS2505 chip once the use counter reached zero. According to Intuitive, “In comparison on IS3000 [S/Si robot] - ISI Key generated from Dallas unique id - key is needed for system to access Dallas data. When instrument is expired, key is wiped. All bits on dallas can only be ‘cleared,’ so once lives ticked off, cannot be reset.”<sup>36</sup> This necessitated development of the Interceptor module and limited repairs to EndoWrists that had at least one use remaining.

35. Based on my conversations with Mr. Hamilton and the deposition transcripts I have reviewed, Rebotix’s Interceptor chip does not affect the communication between the S/Si EndoWrists and the S/Si da Vinci surgical robots. Hospitals report no issues using the S/Si EndoWrists repaired by Rebotix in surgery.<sup>37</sup>

**E. Status of X/Xi Repairs**

36. I understand that Rebotix initially performed a brief investigation of the X/Xi usage counter in 2019, but did not invest significant time or resources into that investigation due to Intuitive’s reaction to Rebotix’s services for the S/Si EndoWrist instruments.<sup>38</sup>

37. Since seeking relief from Intuitive’s conduct, Rebotix has investigated the feasibility of resetting the usage counter on the Xi instruments.<sup>39</sup>

38. I understand that Rebotix has identified two separate ways to extract an image file containing the use counter from the Xi EndoWrist.

---

<sup>36</sup> Intuitive: IS4000 8mm Base Instruments Final Design Review (FDR) Slide 192; Intuitive-00545094.

<sup>37</sup> Harrich Deposition at 34:19 – 38:1. Neither surgeons, first assists, nor scrub assists were able to discern any differences during surgery between Rebotix-repaired EndoWrists and brand new EndoWrists from Intuitive. Harrich Deposition at 38:9 – 39:3.

<sup>38</sup> Interview with Stan Hamilton.

<sup>39</sup> Interview with Stan Hamilton.

## HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

39. One method is detailed in Ms. Mandel's report. It involves using Proxmark 3 (PM3) RFID and Minicom analysis tools in conjunction with crypto libraries and publicly available key lists from CryptoRF investigators to capture and analyze data from the CryptoRF chips. Using these tools and crypto libraries allows communication with the chip and data capture from the chip. The PM3 tool is described by Proxmark as "the tool behind all major RFID Security Research breakthroughs: Mifare Classic Crypto cracking, Mifare PRNG analysis, VingCard exploitation & defeat to name a few."<sup>40</sup> The Minicom tool is a Linux-based serial port emulator that connects devices through serial ports and facilitates the analysis of the captured data.<sup>41</sup> Based on Ms. Mandel's report, her investigation has revealed four features about the CryptoRF chip

- a. The CryptoRF chip does not exhibit any cybersecurity that would prevent writing data to the chip as -adpu commands have been successfully used to bypass authentication.<sup>42</sup>
- b. Initial and follow-up scans have provided no indication that encryption of the EEPROM data at rest is implemented on all sectors of the chip or that unique passwords and keys have been implemented throughout the chip.<sup>43</sup>
- c. Cleartext data has been extracted from the chip.<sup>44</sup>
- d. The image on the chip can be edited and rewritten via an RF link.<sup>45</sup>

---

<sup>40</sup> Proxmark website, <https://proxmark.com/>.

<sup>41</sup> "Getting Started With Minicom", [https://wiki.emacinc.com/wiki/Getting\\_Started\\_With\\_Minicom?gclid=Cj0KCQjw9O6HBhCrARIsADx5qCRdMmNHBNmxMzzPpeC2rsk0rLMkWdEQq1gCFDXfUqN\\_kS5t21Z9Tx0aAt9DEALw\\_wcB](https://wiki.emacinc.com/wiki/Getting_Started_With_Minicom?gclid=Cj0KCQjw9O6HBhCrARIsADx5qCRdMmNHBNmxMzzPpeC2rsk0rLMkWdEQq1gCFDXfUqN_kS5t21Z9Tx0aAt9DEALw_wcB).

<sup>42</sup> Mandel Report at ¶ 20.

<sup>43</sup> Mandel Report at ¶ 20.

<sup>44</sup> Mandel Report at ¶ 23.

<sup>45</sup> Mandel Report at ¶ 27.

## HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

40. These methods are consistent with my experience in conventional RFID tag reverse engineering techniques and are capable of successfully extracting a full image of the CryptoRF EEPROM contents.<sup>46</sup>

41. A second independent path to obtain a full image of the CryptoRF EEPROM is by using a conventional hardware extraction or “dump” of the EEPROM by micro-soldering leads onto the external pins or internal pads of EEPROM block on the chip. This memory “dumping” approach allows direct access to the memory and its contents, bypassing the RF interface, encryption and password engines and other peripheral circuitry. In my experience, this form of conventional hardware extraction is often used when a memory source is otherwise inaccessible. Many EEPROM memories includes a conventional I2C interface because of its 2-wire simplicity, flexibility and adaptability.<sup>47</sup> Because the Atmel CryptoRF EEPROM chip has a conventional 2-wire I2C interface, Rebotix can micro-solder leads to the pads, bypass the RF interface and extract the EEPROM contents. Extracting those EEPROM contents should also produce a clean image file.

42. As detailed in Section 2. D. above, once Rebotix successfully extracted images from the S/Si EndoWrist usage counter, it analyzed those images to locate the usage counter, and then implemented its Interceptor process on the S/Si EndoWrist.

43. The process Rebotix has identified for the Xi EndoWrist usage counter reset is similar to the S/Si EndoWrist process: extracting images, analyzing those images to locate the

---

<sup>46</sup> For example, “The Proxmark III (PM3) is the defacto RFID research tool. There are other alternative tools but none have the community and prevalence of the PM3. It's capable of reading, writing, and emulating many of the currently available RFID tags. In addition, there is a quiet community forum where some highly-technical volunteers share custom Proxmark firmwares and much needed information about RFID research.” “RFID Hacking with The Proxmark 3”, K. Chung, 2017 at <https://blog.kchung.co/rfid-hacking-with-the-proxmark-3/> .

<sup>47</sup> “Advantages and Limitations of I2C Communication”, Total Phase, <https://www.totalphase.com/blog/2016/08/advantages-limitations-i2c-communication/> .



HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

counter, and then implementing a process to reset the Xi usage counter.<sup>48</sup> The process Rebotix is investigating for the Xi EndoWrist usage counter reset should be significantly simpler in that the Xi EndoWrist should not require a CPLD interface device to substitute and bit mask data read from the CryptoRF device or reformat the data to satisfy the X/Xi robot. The CryptoRF chip is reprogrammable unlike the DS2505 which is an add-only memory whose contents cannot be overwritten.<sup>49</sup> Successful extraction and analysis of clean images from the CryptoRF EEPROM facilitates straightforward editing/rewriting of the use count and reprogramming an existing X/Xi EndoWrist CryptoRF EEPROM or replacing the existing CryptoRF EEPROM with a new, CryptoRF EEPROM personalized with the edited image file.<sup>50</sup>

### III. OPINIONS

#### A. Summary of Opinions

44. I have formed three primary opinions after my review of the available information.

45. First, an image will be extracted from the Atmel CryptoRF chip on the X/Xi EndoWrists by Rebotix. The lack of security on the memory portion of the Atmel chip makes the extraction of the image from the chip's memory a simple process. I discuss two methods, an RFID software extraction method and a direct hardwire extraction method, both of which should result in successful image extraction.

46. Second, based on Rebotix's past work with the S/Si EndoWrists and its understanding of the function of the usage counter, it will identify the usage counter in the extracted image. From the initial data pulled from the X/Xi Atmel CryptoRF chip, the memory

---

<sup>48</sup> Interview with Stan Hamilton.

<sup>49</sup> DS2505 Datasheet at 2.

<sup>50</sup> Interview with Stan Hamilton.

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

contents on that chip appears to be virtually identical to the S/Si usage counter. Creating a memory map of the X/Xi usage counter after image extraction would result in an understanding of where the usage counter is and how to reset it.

47. Third, Rebotix will have the capability to implement a reset of the usage counter on the X/Xi EndoWrists. After image extraction, the process of resetting the usage counter on the X/Xi EndoWrists will be easier than resetting the usage counter on the S/Si EndoWrists due to the reprogrammable nature of the CryptoRF chip. This means that the implementation of the Interceptor process would not need to circumvent that bit-wise strike counter, and instead could directly alter the image on the CryptoRF chip to reset the use counter to its original value. Additionally, the X/Xi usage counter is also contained on a chip that can be easily removed from the X/Xi EndoWrist and replaced once with a new CryptoRF chip that can subsequently be reprogrammed multiple times.

**B. An image will be extracted from the Atmel CryptoRF chip on the X/Xi EndoWrists by Rebotix**

*i. Overview of image extraction*

48. Image extraction refers to taking an image contained on a chip's memory and transferring it to a computer or other reader in readable form.

49. An extracted image provides full information about what is stored on the chip, the manner in which the chip's memory is organized, and how the functions that can be performed by the chip operate.

*ii. Process of image extraction*

50. Several security methods can make the extraction of an image from the memory of a chip more difficult. First, if the data on the chip itself is encrypted, the image extracted from the chip would first need to be decrypted before being readable. Second, hardware security

could be implemented on the chip to prevent external hardware connections from attempting to extract data. Third, physical anti-tampering mechanisms can be employed to make reverse engineering efforts such as dying, scanning probes, and voltage contrast methods more difficult to implement.<sup>51</sup>

51. By contrast, if there are no security methods implemented on the actual memory portion of the chip, extracting a full image is straightforward, and can be accomplished using multiple different methods depending on how the chip communicates.

52. If a chip communicates via a hardwire connection and has no additional security, an image can be extracted from the chip's memory using a simple hardwire connection. A hardwire connection to the chip's external pins or internal pads allows for the chip's memory contents to be read directly.<sup>52</sup>

53.. If a chip communicates using an RFID link, the same hardwire connection method is possible. For the Atmel CryptoRF chip, where the section of the chip responsible for communicating data via an RF link is separate from the memory that contains the data to be transferred, this hard-wire connection involves a direct connection to the EEPROM memory. And none of the security measures that I identified above appear to be in use or active to secure that EEPROM memory.

iii. *Extraction from the Atmel CryptoRF chip on the da Vinci Xi EndoWrists*

54. As discussed above, the Atmel CryptoRF chip used on the da Vinci Xi EndoWrist does not have active security implemented on the memory portion of the chip that

---

<sup>51</sup> "Use an External Encrypted EEPROM to Secure Data in Embedded Systems" Digi-Key, <https://www.digikey.com/en/articles/use-external-encrypted-eprom--secure-data-embedded-systems>.

<sup>52</sup> Extended Learning Institute (ELI) at Northern Virginia Community College (NOVA). "Introduction to Computer Applications and Concepts." *Lumen*, [courses.lumenlearning.com/zeliite115/chapter/reading-read-only-memory/](https://courses.lumenlearning.com/zeliite115/chapter/reading-read-only-memory/).

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

stores the image. The only implemented security activates when the RFID portion of the Atmel CryptoRF chip communicates with the da Vinci robot.

55. Rebotix has investigated two methods for extracting the image from the Atmel CryptoRF chip. One method operates via an RFID connection to the chip. The other operates through a hard-wire connection to the EEPROM memory on the CryptoRF chip.

*iv. RFID Method*

56. The methodology described by Ms. Mandel in her report resulted in a connection to the Atmel CryptoRF chip, the establishment of bi-directional communication, and the transmission of data from the Atmel chip to the reader.

57. The data retrieved from the chip by Ms. Mandel was not in any way encrypted or otherwise secured. This is what is referred to as “clear data.” A chip’s image consists of the clear data with a particular organization.

58. Because the connection with the chip has resulted in the communication of clear data, the full unencrypted image can be extracted from the chip. The communication of clear data means that any security on the communication and any security on the actual data itself has been overcome. When data extraction methods result in clear data being extracted, the only step that remains before full image extraction is some additional time. An unencrypted (clear text) binary image file is readily convertible to usable, editable text using a standard hex editor.<sup>53</sup>

*v. Hard Wire Method*

59. In parallel to Ms. Mandel’s method, it is my understanding that Rebotix is extracting the image from the Atmel CryptoRF chip using a hard wire connection to the actual

---

<sup>53</sup> 010 Editor Manual - Using the Hex Editor, [www.sweetscape.com/010editor/manual/UsingHexEditor.htm](http://www.sweetscape.com/010editor/manual/UsingHexEditor.htm).

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

EEPROM memory in the chip.<sup>54</sup> This method bypasses any RFID link entirely and allows for direct access to the memory image.

60. This method is commonly used in the data security and extraction field to retrieve data directly from memory devices.<sup>55</sup>

61. With a direct hardwire connection, if there are no physical anti-tampering security measures, full image extraction occurs over the direct connection to the chip's memory. And here, there are no security measures on the chip's memory that inhibit a hardwire extraction.<sup>56</sup>

**C. The usage counter in the extracted image will be identified by Rebotix**

*i. Analyzing an extracted image*

62. After an image is extracted from a memory device, that image is analyzed to determine how it is structured. In my experience as a reverse engineer, this process of image analysis is simple as long as the underlying image does not have additional encryption.

63. The generally accepted steps to perform a binary image analysis involve using a binary image scanning tool such as binwalk and an open-source binary file scanner. Using those two tools in conjunction with a hex editor, binary data is converted into individual files and the overall file structure and organization of an image is established. This process converts a binary image into readable, editable files.<sup>57</sup>

64. Every conventional digital memory is a device that stores bits (i.e. 1's and 0's) in an organized fashion. A full binary image of the memory includes all of the individual bits

---

<sup>54</sup> Interview with Stan Hamilton

<sup>55</sup> Fukami, Aya, et al. "A New Model for Forensic Data Extraction from Encrypted Mobile Devices." *Forensic Science International: Digital Investigation*, Elsevier, 27 May 2021, [www.sciencedirect.com/science/article/pii/S2666281721000779](https://www.sciencedirect.com/science/article/pii/S2666281721000779).

<sup>56</sup> Atmel CryptoRF EEPROM Memory Full Specification at 35.

<sup>57</sup> Canonical. *Ubuntu Manpage: Binwalk - Binary Image Search Tool*, [manpages.ubuntu.com/manpages/trusty/man1/binwalk.1.html](https://manpages.ubuntu.com/manpages/trusty/man1/binwalk.1.html).

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

that are stored in the memory. Binary analysis then organizes or structures those bits into recognizable groups that represent individual files. Once those bits are organized, then the files can be read, their functions identified, and their values edited. This structural analysis provides an understanding of how the memory on the chip is programmed and how the chip fulfills its required function. All of a memory device's information is necessarily contained in that image.

*ii. The extracted image from the Atmel CryptoRF chip*

65. The image on the Atmel CryptoRF chip on the da Vinci EndoWrist fulfills two primary required functions. First, the image contains information that identifies the model of EndoWrist.<sup>58</sup> Second, the image contains the use counter and the number of remaining uses on the use counter.

66. The Atmel AT88SC6416 CryptoRF RFID chip contains 8,192 bytes of User Memory equally divided into 16 user zones of 512 bytes each.<sup>59</sup> Ms. Mandel has analyzed the data contained in each User Zone and determined that [REDACTED] contains the use counter and other relevant information about the Xi EndoWrist.<sup>60</sup> This allows Rebotix to focus only on the User Zone data from [REDACTED] to determine which data in that zone need to be edited in order to produce an image file consistent with the original number of uses on the use counter.

*iii. Ms. Mandel's investigation has identified the location of the usage counter*

67. Ms. Mandel describes an analysis of the User Zones on the Atmel CryptoRF chip.<sup>61</sup> In that analysis, Ms. Mandel identified the User Zone that contains relevant information

<sup>58</sup> Intuitive Surgical da Vinci Xi System User Manual at E-16, "RFID communication is used by the da Vinci Xi system to detect and identify instruments and endoscopes that are installed on the system."

<sup>59</sup> Atmel CryptoRF EEPROM Memory Full Specification, Tables 3-1 and C-6.

<sup>60</sup> Mandel Report at ¶ 17.

<sup>61</sup> Mandel Report at ¶ 17.

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

about the model of the EndoWrist and its serial number.<sup>62</sup> Further, Ms. Mandel identified the User Zone that contains the relevant information about the usage counter.<sup>63</sup>

68. Ms. Mandel's ability to identify these specific pieces of information in the image demonstrates that the precise location of the usage counter on the image can be readily identified. And because Ms. Mandel has already narrowed the location of the use counter to a particular User Zone, Rebotix can isolate the use counter function on that zone.

*iv. Several additional factors make the process of Rebotix's image analysis for the Xi EndoWrist CryptoRF chip easier than others that I have encountered in my career*

69. Generally, in my experience, when a reverse engineer encounters an image for the first time, that engineer will not have prior experience with that image.

70. Prior experience with similar images and functions of similar chips makes the process of image analysis easier.

71. If two chips have similar or identical images, prior analysis of the image of the first of the two chips (Chip A) makes the analysis of the second chip (Chip B) simpler. Even if the initial analysis of Chip A takes significant time and resources, image analysis on Chip B can use the foundational understanding of Chip A's image.

72. Further, if two chips fulfill similar or identical functions, understanding the manner in which one function is implemented in a chip's image provides an understanding of how that function is implemented in another chip's image, even if there are differences between the images themselves.

---

<sup>62</sup> Mandel Report at ¶ 17.

<sup>63</sup> Mandel Report at ¶ 17.

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

73. Rebotix already created a memory map of the S/Si EndoWrist usage counter when it developed the Interceptor process for the S/Si EndoWrist.<sup>64</sup> This gave Rebotix an understanding of the memory structure, how data pulled from the chip is organized, and what portions of the S/Si chip's memory contained the usage counter.<sup>65</sup>

74. This work established both a direct understanding of the image and an understanding of how the usage counter function was implemented on that chip's memory architecture.

75. The Atmel CryptoRF chip has significant functional similarity, because it implements the same usage counter function as the S/Si. The chip decreases the number of available uses by one after an Xi EndoWrist is used in surgery.<sup>66</sup> An understanding of how that function was implemented in the S/Si EndoWrist usage counter makes understanding that implementation in the Xi image simpler.

76. Moreover, the data retrieved by Ms. Mandel from the Atmel CryptoRF chip on the Xi EndoWrist is highly similar or identical to the data that Rebotix extracted from the Dallas chip on the S/Si EndoWrists.<sup>67</sup> This similarity between the data extracted from the Xi EndoWrist and prior data analyzed by Rebotix on the S/Si EndoWrist makes image analysis a straightforward process.

---

<sup>64</sup> Interview with Stan Hamilton.

<sup>65</sup> Interview with Stan Hamilton.

<sup>66</sup> McGrogan Deposition at 78:10-18.

<sup>67</sup> Interview with Stan Hamilton.



HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

**D. Rebotix can use the extracted image to reset the usage counter on da Vinci Xi EndoWrists**

77. In my professional experience, once an image has been extracted from an EEPROM chip, analyzed, and converted to a hexadecimal file, an EEPROM programmer can use that hex file to reprogram the existing EEPROM or program a new replacement EEPROM. This general process of extraction and reprogramming is a basic methodology that has been successfully used in the reverse engineering of commercial EEPROM memories for many years.<sup>68</sup>

*i. There are two approaches to reset the usage counter on the Xi EndoWrist*

78. The first is to utilize Ms. Mandel's method of establishing an RFID connection with the appropriate authentication and keys and writing new values to the User Zone.

79. The second is to modify the extracted image, return the use counter to its original state, write that image to a new Atmel CryptoRF chip, and replace the original chip on the Xi EndoWrist with the new chip.

*ii. RFID Connection Writing*

80. Ms. Mandel's methodology was successful in issuing 14a and 14b commands to the Atmel CryptoRF chip. Ms. Mandel also successfully established a direct connection with the User Zone section of the memory image and both sent data to and received data from that User Zone.

81. With the extracted image identified and organized, sent data can modify that portion of the image that contains the remaining value on the usage counter.

---

<sup>68</sup> Conti, Gregory, et al. "Visual Reverse Engineering of Binary and Data Files." *Visualization for Computer Security Lecture Notes in Computer Science*, Sept. 2008, pp. 1–17., doi:10.1007/978-3-540-85933-8\_1.

## HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

82. Intuitive's description of the use counting data areas being one-time programmable and unable to be modified once written do not change my conclusion.<sup>69</sup> Ms. Mandel was able to access the User Zone and establish direct read/write command communication.

83. The actual modification of the count set on the usage counter does not require a new write of an entire image to the usage counter. Instead, it merely requires the remaining value of the usage counter to be adjusted. Ms. Mandel's analysis of the CryptoRF User Memory has further confirmed that the stored code is small and confined to a single user zone. The use counter value on that user zone consists of only a few bits of data specifying the remaining uses. There are multiple reasons that the portion of the use counter that stores the number of uses is modifiable via an RFID connection.

84. First, the actual value remaining on the use counter has to be changed after being used in surgery. When the da Vinci X or Xi robot establishes a connection with the robot, it reads the value on the usage counter.<sup>70</sup> And it must also be able to cause that usage counter value to change after it is used in surgery.<sup>71</sup> Because the value of the usage counter is variable by the very nature of its function, that value is capable of being changed.

85. Second, Ms. Mandel's method indicates that once the appropriate connection with the Atmel CryptoRF chip is established, read/write commands can be freely issued to and are received by the chip.<sup>72</sup> Those commands include hex commands, and commands to alter data present on the chip.<sup>73</sup> Based on my review of Ms. Mandel's report and her ability to have

---

<sup>69</sup> Intuitive-00506542.

<sup>70</sup> Intuitive-00552746; Intuitive-00593473.

<sup>71</sup> Intuitive-00593477- Intuitive-00593478.

<sup>72</sup> Mandel Report at ¶¶ 25-26.

<sup>73</sup> Mandel Report at ¶¶ 26-27.

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

those commands issued and received, there is no barrier to writing new values to the usage counter on the chip once an RF connection is successfully established.

86. Third, there is no additional encryption or security barrier that prevents writing new data to the chip. As discussed previously, the extraction of clear data from the chip once an RFID connection has been established indicates that there are no additional barriers to writing data. As discussed previously, the data stored in the CryptoRF EEPROM memory is not encrypted and there are no additional physical security features on the chip to prevent extraction of a clean image file.

87. Fourth, the encryption keys are “behind” the security fuses and will also be directly extracted as part of the EEPROM image file and therefore accessible to Rebotix. The CryptoRF datasheet states that “These [security] fuses do not control access to the user memory; user memory access rights are defined in the Access Registers. The security fuses are used to lock the state of the Access Registers, Passwords, Keys, and other configuration data during the personalization process so that they cannot be changed after a card is issued.” Since the use counter data by definition must be allowed to change as a function of EndoWrist use, it cannot be a value locked by a security fuse.

*iii. Hardware Chip Replacement*

88. A second approach to resetting the usage counter involves adjusting the usage counter value on the extracted image, copying that image to a new blank Atmel CryptoRF chip, and installing that Atmel CryptoRF chip back into the Xi EndoWrist.

89. Based on Ms. Mandel’s report, the Atmel CryptoRF chips have some specific identifying information (such as serial numbers and model of EndoWrist), but the remaining image is identical.

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

90. Adjusting the image after it has been extracted to reset the usage counter involves altering the bits of data that specify the current use counter value and returning them to their original number of uses. The original EndoWrist device has a published specification on the initial value of the usage counter.<sup>74</sup> Adjusting the image would involve modifying the bits of data to correspond to the original published specification for the number of uses.

91. After the image is adjusted to reset the usage counter to its original value, that image can be written to a blank Atmel CryptoRF chip. The image would be identical to an original Atmel CryptoRF chip included on the Xi EndoWrist, with a reset number of uses to the original use count. And because EndoWrists function regularly with a use counter showing that original value, the new chip would cause the repaired EndoWrist to function just as a brand new EndoWrist would.

92. Nothing about the image or the general structure of the Atmel CryptoRF chip precludes this type of image rewrite to a new chip. And the design of the Xi EndoWrist does not preclude removing the Atmel CryptoRF chip and installing a new chip containing the new image. In fact, due to the inherent reprogrammable nature of the CryptoRF chips, the chip replacement repair process should only be necessary once, allowing for the X/Xi EndoWrist to be repaired multiple times without further chip replacement.<sup>75</sup>

#### IV. OTHER ISSUES

##### A. Intuitive's own security testing

93. Based on documentation from Intuitive, it appears that Intuitive engaged a third party to investigate potential security issues with the RFID system used on the da Vinci

---

<sup>74</sup> Intuitive-00671027; Intuitive-00671034.

<sup>75</sup> Interview with Stan Hamilton.

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

X/Xi.<sup>76</sup> In that report, prepared in November of 2013, the third party conducted testing on the RFID system using a standard RFID reader/writer programming device.<sup>77</sup> As part of that testing,

the [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]<sup>79</sup>

94. This outdated report does not change my opinion for four reasons.

95. First, the methods and technology used [REDACTED]

[REDACTED] The report describes the custom [REDACTED]

[REDACTED]<sup>80</sup> This setup is a [REDACTED]

[REDACTED] Because the Atmel CryptoRF includes security that becomes active when a direct RFID connection is established in this manner, it is unsurprising that [REDACTED]

[REDACTED]

96. Second, the described tests used a flawed and outdated methodology for accessing the Atmel chip. Based on the description provided in the report, [REDACTED]

s [REDACTED]<sup>81</sup> [REDACTED], there

<sup>76</sup> Intuitive-00506582 (Cylance Professional Services Technical Report).

<sup>77</sup> Intuitive-00506593 – Intuitive-00506594.

<sup>78</sup> Intuitive-00506594.

<sup>79</sup> Intuitive-00506594.

<sup>80</sup> Intuitive-00506593.

<sup>81</sup> Intuitive-00506593 – Intuitive-00506594.

HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

is no way to customize the RFID connection to transmit proper authentication keys or protocols. Both Authentication Communication and Encryption Communication modes in the CryptoRF chip are “activated by performing Mutual Authentication between the host system and the PICC using the Verify Crypto command.”<sup>82</sup> This means that the Xi robot (the host) and the CryptoRF chip (the PICC) must share encrypted passwords that a simple RFID reader could not decrypt. The method employed by Ms. Mandel used a sniffing method to monitor data being transferred before attempting to make direct reads and writes to the device.<sup>83</sup> This observation of initially transmitted data is an important step that allowed Ms. Mandel to establish a two-way connection with the Atmel CryptoRF chip and extract data from the chip. [REDACTED]

[REDACTED]

97. Third, the [REDACTED]

[REDACTED] The report did not discuss any security implemented on the chip that would prevent this type of hard-wire connection.

98. [REDACTED]

[REDACTED] As discussed above, there is no implemented security method that prevents this approach from being successful.

Executed on July 26, 2021,

  
Kurt Humphrey

---

<sup>82</sup> Atmel Crypto RF EEPROM Memory Full Specification Datasheet Appendices J, K.

<sup>83</sup> Mandel Expert Report at ¶ 17.

### Exhibits 1

- Interview with Stan Hamilton on 7/23/21
- June 7<sup>th</sup>, 2021, Deposition of Anthony McGrogan
- June 4<sup>th</sup>, 2021, Deposition of Stan Hamilton
- Atmel CryptoRF EEPROM Memory Full Specification
- Dallas Semiconductor DS2505 Data Sheet
- Da Vinci X Manual
- Da Vinci Xi Manual
- Intuitive-00506505-Intuitive-00506641
- Intuitive-00512348-Intuitive-00512353
- Intuitive-00544903-Intuitive-00545124
- Intuitive-00552745-Intuitive-00552759
- Intuitive-00593443-Intuitive-00593480
- Intuitive-00671020-Intuitive-00671035
- Expert Report by Gwen Mandel
- Fukami, Aya, et al. “A New Model for Forensic Data Extraction from Encrypted Mobile Devices.” *Forensic Science International: Digital Investigation*, Elsevier, 27 May 2021, [www.sciencedirect.com/science/article/pii/S2666281721000779](http://www.sciencedirect.com/science/article/pii/S2666281721000779).
- Conti, Gregory, et al. “Visual Reverse Engineering of Binary and Data Files.” *Visualization for Computer Security Lecture Notes in Computer Science*, Sept. 2008, pp. 1–17., doi:10.1007/978-3-540-85933-8\_1.